#2

Docket No. 1080.1088/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Yusuke KAWASAKI, et al.

Serial No.: To Be Assigned

Group Art Unit: To Be Assigned

Examiner: To Be Assigned

Filed: December 18, 2000

For: PROCESSING APPARATUS AND INTEGRATED CIRCUIT

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-212815, filed July 13, 2000.

It is respectfully requested that Applicants be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Dated: December 18, 2000

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ７月１３日

出 願 番 号
Application Number: 特願２０００－２１２８１５

出 願 人
Applicant (s): 富士通株式会社

２０００年１０月１３日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３０８４６１９

【書類名】　特許願

【整理番号】　0051226

【提出日】　平成12年 7月13日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　9/00

G09C　1/00

【発明の名称】　処理装置および集積回路

【請求項の数】　20

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　川▲崎▼　雄介

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　櫻井　博

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　橋本　繁

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　山本　浩憲

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100094330

【弁理士】

【氏名又は名称】　山田　正紀

【選任した代理人】

【識別番号】　100109689

【弁理士】

【氏名又は名称】　三上　結

【手数料の表示】

【予納台帳番号】　017961

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9912909

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　処理装置および集積回路

【特許請求の範囲】

【請求項１】　プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、前記ＣＰＵと前記内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

前記バスラインの、外部に延びた部分に外付けされた、各所定の作用を成す１つ以上の外部デバイスを含む外部回路を備え、

前記内部回路が、前記バスラインの、外部への出入口に介在し、該バスライン上のアドレスおよびデータを、前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部を含むものであることを特徴とする処理装置。

【請求項２】　前記外部回路が複数の外部デバイスを含むものであり、

前記暗号化部は、前記複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることを特徴とする請求項１記載の処理装置。

【請求項３】　前記暗号化部は、前記外部回路がアクセスされていないタイミングで、前記バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることを特徴とする請求項１記載の処理装置。

【請求項４】　前記ＣＰＵは、クロックの供給を受け供給されたクロックに同期してプログラムを実行するものであるとともに、前記暗号化部も、クロックの供給を受け供給されたクロックに同期して暗号化を行なうものであって、

前記暗号化部に、前記ＣＰＵに供給されるクロックよりも高速なクロックを供給するクロック供給部を備えたことを特徴とする請求項１記載の処理装置。

【請求項５】　前記外部回路の構成を認識し、その構成に応じて、前記暗号化部における暗号化パターンを決定する暗号化パターン決定手段を有することを特徴とする請求項１記載の処理装置。

【請求項６】　前記暗号化部は、前記バスライン上のアドレスおよびデータを、前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じるとともに前記ＣＰＵで実行されるアプリケーションプログラ

ムにも応じた暗号化パターンで暗号化するものであることを特徴とする請求項１記載の処理装置。

【請求項７】　前記バスラインの、外部に延びた部分に接続され、該バスライン上の暗号化されたアドレスおよびデータを暗号化前のアドレスおよびデータに戻す逆暗号化部を備えたことを特徴とする請求項１記載の処理装置。

【請求項８】　前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することを特徴とする請求項１記載の処理装置。

【請求項９】　前記暗号化部は、前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることを特徴とする請求項１記載の処理装置。

【請求項１０】　プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、前記ＣＰＵと前記内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

前記バスラインの、外部に延びた部分に外付けされた、情報を記憶するメモリを含む外部回路を備え、

前記内部回路が、前記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする処理装置。

【請求項１１】　前記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることを特徴とする請求項１０記載の処理装置。

【請求項１２】　前記メモリに記憶された情報のうちの少なくとも一部の情報が、前記所定の初期化動作を実行する以前において既に暗号化されたものであって、

前記情報書換手段は、該少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであること

を特徴とする請求項１０記載の処理装置。

【請求項１３】　前記内部回路が前記暗号化部で採用される暗号化パターンを保持してなるものであって、

タンパ検出を行なうタンパ検出部を備えるとともに、

前記タンパ検出部によるタンパ検出を受けて前記内部回路内に保持されていた暗号化パターンを破壊する暗号化パターン破壊手段を備えたことを特徴とする請求項１又は１０記載の処理装置。

【請求項１４】　プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、前記ＣＰＵと前記内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、各所定の作用を成す１つ以上の外部デバイスが外付けされる、アドレスおよびデータを伝達するバスラインと、該バスラインの、外部への出入口に介在し、該バスライン上のアドレスおよびデータを、該バスラインの、外部に延びた部分に外付けされた１つ以上の外部デバイス全体に割り当てられた空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部とが搭載されてなることを特徴とする集積回路。

【請求項１５】　前記バスラインの、外部に延びた部分に、複数の外部デバイスが外付けされた場合に、前記暗号化部は、前記複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることを特徴とする請求項１４記載の集積回路。

【請求項１６】　前記暗号化部は、前記外部回路がアクセスされていないタイミングで、前記バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることを特徴とする請求項１４記載の集積回路。

【請求項１７】　前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することを特徴とする請求項１４記載の集積回路。

【請求項１８】　前記暗号化部は、前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して

データを暗号化するものであることを特徴とする請求項１４記載の集積回路。

【請求項１９】　プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、前記ＣＰＵと前記内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、情報を記憶するメモリが外付けされる、アドレスおよびデータを伝達するバスラインとを備えるとともに、

前記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする集積回路。

【請求項２０】　前記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることを特徴とする請求項１９記載の集積回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＣＰＵおよび内部デバイスを有する内部回路と、その内部回路に対し外付けされた外部デバイスを含む外部回路とを備えた処理装置、および、ＣＰＵおよび内部デバイスが搭載されるとともにに外部デバイスの外付けが可能な集積回路に関する。

【０００２】

【従来の技術】

近年のＬＳＩ技術の発達により、プログラムを実行するＣＰＵや、そのＣＰＵで実行されるプログラムが格納されるメモリや、さらに他の様々なデバイスを１つのチップ上に集積することができるようになり、装置の小型化、低コスト化等に大きく貢献している。このようなＬＳＩを製造するにあたり、ユーザによらず同一のプログラムを実行するシステムであって、かつ完成したあと途中でプログラムを変更する必要がないシステムについてはＬＳＩチップ上にプログラムを記憶したメモリを搭載しておけばよいが、ユーザに応じて異なるプログラムを実行させたり、あるいは、使用している途中でプログラムを変更する必要がある場合、上記のような構成のＬＳＩにさらに外部メモリを外付けすることができるよう

に構成しておき、使用している途中で変更する可能性のあるプログラム、あるいはユーザに応じて異なるプログラムはその外付けの外部メモリに記憶するようにしておくことが望ましい。

【０００３】

【発明が解決しようとする課題】

ところが、そのような外部メモリを外付けることができるシステムの場合、その外部メモリの内容が不正に書き換えられたり、あるいはその外部メモリが、その外部メモリと同一仕様の、不正なプログラムを記憶したメモリに差し替えられてしまい、内部のメモリに記憶されている重要なプログラムやデータが不正にアクセスされ、その重要なプログラムやデータの内容が不正に解読されてしまう危険性がある。以下に、一例を挙げる。

【０００４】

近年、急速に現金価値や現金相当のポイント価値をデータとしてもつＩＣカードや磁気カードが普及しつつあり、それに伴って、カードの偽造や変造を防止するための対策としてデータのセキュリティ確保が急務となってきている。これに対処するために、過去においても装置の逆解析（リバースエンジニアリング）を防ぐ方法が試みられてきたが、それらの試みにもかかわらず裏ＲＯＭ等が作成され、装置が開発者の不本意な用途に悪用されることが絶えないのが現状である。

【０００５】

本発明は、上記事情に鑑み、不正なアクセスや逆解析の防止が図られた処理装置および集積回路を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上記目的を達成する本発明の処理装置のうちの第１の処理装置は、

プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、ＣＰＵと内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

上記バスラインの、外部に延びた部分に外付けされた、各所定の作用を成す１つ以上の外部デバイスを含む外部回路を備え、

上記内部回路が、上記バスラインの、外部への出入口に介在し、そのバスライン上のアドレスおよびデータを、上記の１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部を含むものであることを特徴とする。

【０００７】

ここで、上記暗号化部で採用される暗号化パターンには、アドレスおよびデータの双方とも暗号化しないことも１つの暗号化パターンとして含まれる。

【０００８】

このように、アドレス空間を複数に分割し、その分割した各領域ごとに異なったパターンで暗号化することにより、暗号化の解析が困難となる。

【０００９】

上記本発明の第１の処理装置において、上記外部回路が複数の外部デバイスを含むものであり、

上記暗号化回路は、上記複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることが好ましい。

【００１０】

こうすることにより、例えば外部デバイスの１つとしてフラッシュＲＯＭを備えた場合は、そのフラッシュＲＯＭに関してはアドレスとデータとの双方を暗号化し、外部デバイスの１つとして連続アドレスについて高速読出しが可能なＲＡＭについては性能を落とさないようにデータのみ暗号化するか、あるいはアドレスについても暗号化するものの、連続読出しの行なわれる、アドレスの下位ビット側は暗号化しないようにし、外部デバイスの１つとしてＩ／Ｏデバイスを備えた場合は、アドレス、データとも暗号化しないなど、その外部デバイスの性質に合わせた暗号化を行なうことができる。

【００１１】

また、上記本発明の第１の処理装置において、上記暗号化部は、外部回路がアクセスされていないタイミングで、バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることが好ましい。

【００１２】

こうすることにより不正な解析が一層難しくなる。

【００１３】

また、上記本発明の第１の処理装置において、上記ＣＰＵは、クロックの供給を受け供給されたクロックに同期してプログラムを実行するものであるとともに、上記暗号化部も、クロックの供給を受け供給されたクロックに同期して暗号化を行なうものであって、上記暗号化部に、ＣＰＵに供給されるクロックよりも高速なクロックを供給するクロック供給部を備えることがが好ましい。

【００１４】

こうすると、複雑な暗号化が可能になる。

【００１５】

さらに、上記本発明の第１の処理装置において、外部回路の構成を認識し、その構成に応じて、暗号化部における暗号化パターンを決定する暗号化パターン決定手段を有することが好ましい。

【００１６】

この暗号化パターン決定手段を持つことにより、外部回路の構成が異なるごとにオペレータがいちいち暗号化パターンを決定するといった作業が不要となる。

【００１７】

さらに、上記本発明の第１の処理装置において、上記暗号化部は、上記バスライン上のアドレスおよびデータを、上記の１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じるとともにＣＰＵで実行されるアプリケーションプログラムにも応じた暗号化パターンで暗号化するものであることが好ましい。

【００１８】

これにより、暗号化のパターンが一層複雑となり、不正な解析が一層困難となる。

【００１９】

さらに、上記本発明の第１の処理装置において、上記バスラインの、外部に延びた部分に接続され、バスライン上の暗号化されたアドレスおよびデータを暗号化前のアドレスおよびデータに戻す逆暗号化部を備えることが好ましい。

【００２０】

この逆暗号化部を備えないままデバッグを行なおうとするとアドレスやデータが暗号化されているためデバッグが極めて困難になる。そこで、この逆暗号化部を備えることにより、装置の開発時に容易にデバッグを行なうことができる。

【００２１】

この逆暗号化部は、デバッグが済んだ後は不要であり、処理装置から取り外され、あるいは動作不能な状態に固定あるいは破壊されることが望ましい。

【００２２】

さらに、上記本発明の第１の処理装置において、上記の１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することが好ましい。

【００２３】

所定の初期化動作、例えば電源投入時やリセット時等に暗号化パターンを再設定することにより、不正な解析が一層困難になり、セキュリティが一層向上する。

【００２４】

さらに、上記本発明の第１の処理装置において、上記暗号化部は、上記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることが好ましい。

【００２５】

このように、データを暗号化するときの暗号化関数としてアドレスの関数を採用することにより、複雑な暗号化が可能となり、不正な解析が一層困難となり、データのセキュリティが一層向上する。

【００２６】

また本発明の処理装置のうちの第２の処理装置は、

プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、ＣＰＵと内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデー

タを伝達するバスラインとを含む内部回路、および

上記バスラインの、外部に延びた部分に外付けされた、情報を記憶するメモリを含む外部回路を備え、

上記内部回路が、上記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする。

【００２７】

ここで上記所定の初期化動作とは、典型的には、最初の電源投入時の初期化動作である。

【００２８】

このように、例えば最初の電源投入時の初期化動作等、所定の初期化動作で、メモリの内容を暗号化して書き換えることにより、データのセキュリティが一層向上する。

【００２９】

この場合に、上記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることが好ましい。

【００３０】

この場合、処理装置のメーカ側の人間を含め、誰もが知らない暗号化パターンで情報が暗号化されることになり、データのセキュリティがさらに向上する。

【００３１】

ここで、上記第２の処理装置において、上記メモリに記憶された情報のうちの少なくとも一部の情報が、上記の所定の初期化動作を実行する以前において既に暗号化されたものであって、

上記情報書換手段は、その少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであることも好ましい形態である。

【００３２】

この場合に、上記の少なくとも一部の情報を暗号化前の情報に戻すための復号化情報が上記メモリに記憶されてなるものであって、

上記情報書換手段は、その少なくとも一部の情報を、その復号化情報を用いて一旦暗号化前の情報に戻すものであってもよい。

【００３３】

このように、工場出荷時には別の暗号化パターンで暗号化しておくことによりセキュリティがさらに向上する。

【００３４】

また、上記のように、工場出荷時に別の暗号化パターンで暗号化しておくにあたっては、上記の少なくとも一部の情報が公開鍵により暗号化されたものであるとともに、この処理装置は秘密鍵が埋め込まれてなるものであって、

上記情報書換手段は、その少なくとも一部の情報をその秘密鍵を用いて一旦暗号化前の情報に戻すものであってもよく、あるいは上記の少なくとも一部の情報を暗号化前の情報に戻すための、暗号化された形式の復号化情報を外部より取得する情報取得部を備え、

上記情報書換手段は、情報取得部で取得された、暗号化された形式の復号化情報を復号化して平文の復号化情報を取り出しこの平文の復号化情報を用いて上記の少なくとも一部の情報を一旦暗号化前の情報に戻すものであってもよい。

【００３５】

暗号化パターンとして公開鍵を用い、その公開鍵で暗号化された情報をメモリに書き込んでおき、内部に埋め込まれた秘密鍵で暗号化前の情報に戻すようにすると、例えば同一仕様の処理装置を複数の会社等で使用した場合に、各会社に公開鍵のみを渡すことにより、会社間のセキュリティが確保できる。

【００３６】

また、復号化情報を外部より取得できるように構成すると、例えば通信等により鍵管理センター等から復号化情報を入手することが可能となり、柔軟なシステム構成が可能となる。

【００３７】

さらに、上記第２の処理装置において、上記内部回路が上記暗号化部で採用される暗号化パターンを保持してなるものであって、

タンパ検出を行なうタンパ検出部を備えるとともに、

上記タンパ検出部によるタンパ検出を受けて上記内部回路内に保持されていた暗号化パターンを破壊する情報破壊手段を備えることが好ましい。

【００３８】

この処理装置を不正にこじ開けたり分解しようとしたときにタンパ検出がなされ、そのタンパ検出を受けて暗号化パターンを破壊することにより、不正な解読がますます困難になり、セキュリティの一層の向上に寄与することになる。

【００３９】

また、上記目的を達成する本発明の集積回路のうちの第１の集積回路は、プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、ＣＰＵと内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、各所定の作用を成す１つ以上の外部デバイスが外付けされる、アドレスおよびデータを伝達するバスラインと、そのバスラインの、外部への出入口に介在し、そのバスライン上のアドレスおよびデータを、そのバスラインの、外部に延びた部分に外付けされた１つ以上の外部デバイス全体に割り当てられた空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部とが搭載されてなることを特徴とする。

【００４０】

本発明の第１の集積回路は、上記の構成を有するものであり、本発明の第１の処理装置と同一の作用効果を奏するとともに、集積回路（ＬＳＩ）であることからその回路構成等の解析が困難であり、この点からもセキュリティの向上に寄与している。

【００４１】

ここで、上記第１の集積回路において、上記の本発明の第１の処理装置と同様、上記暗号化部で採用される暗号化パターンには、典型的には、アドレスおよびデータの双方とも暗号化しないことも１つの暗号化パターンとして含まれており、また、上記バスラインの、外部に延びた部分に、複数の外部デバイスが外付けされた場合に、暗号化部は、それら複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることが好ましく、

また、上記暗号化部は、外部回路がアクセスされていないタイミングで、上記

バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることも好ましい形態であり、

さらに、上記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することも好ましい形態であり、

さらに、上記暗号化部は、上記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることも好ましい形態である。

【００４２】

また、本発明の集積回路のうちの第２の集積回路は、プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、ＣＰＵと内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、情報を記憶するメモリが外付けされる、アドレスおよびデータを伝達するバスラインとを備えるとともに、上記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする。

【００４３】

本発明の第２の集積回路は、上記の構成を有するものであり、本発明の第１の処理装置と本発明の第１の集積回路との関係と同様、本発明の第２の処理装置と同一の作用効果を奏するものであり、さらに集積回路（ＬＳＩ）であることからその回路構成等の解析が困難であり、この点からもセキュリティの向上が図られている。

【００４４】

ここで、上記第２の集積回路において、上記本発明の第２の処理装置と同様、上記所定の初期化動作は、典型的には、最初の電源投入時の初期化動作であり、

また、上記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることが好ましく、

さらに、上記メモリに記憶された情報のうちの少なくとも一部の情報が、上記の所定の初期化動作を実行する以前において既に暗号化されたものであって、

上記情報書換手段は、その少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであることも好ましい形態である。

【００４５】

尚、本発明においては、１つの暗号化演算方式を本発明にいう暗号化パターンの１つとしてとらえ、暗号化演算方式が異なることをもって暗号化パターンが異なるものとしてもよく、暗号化演算方式は共通であって、その暗号化演算方式において用いられる変数等が異なることをもって暗号化パターンが異なるものとしてもよい。

【００４６】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

【００４７】

図１は、本発明の処理装置の第１実施形態を示すブロック図である。

【００４８】

この図１に示す処理装置１は、ＬＳＩ１０の内部に搭載された内部回路１００と、ＬＳＩ１０の外部に外付けされた外部回路２００と、その他発振器３０１，３０２等から構成されている。このＬＳＩ１０は、本発明の集積回路の一実施形態にも相当する。

【００４９】

ＬＳＩ１０の内部に構成された内部回路１００は、中央処理装置（ＣＰＵ）１０１、および、それぞれが、本発明にいう内部デバイスである、内部メモリ１０２、暗号化情報レジスタ１０３、アドレスデコーダ１０４、およびその他の周辺回路１０５を有する。ＣＰＵ１０１および各種の内部デバイスは、バスライン１１０で相互に接続されている。このバスラインは、アドレスバス１１１とデータバス１１２とで構成され、ＬＳＩ１０の外部にまで延びている。このバスライン１１０の、外部にまで延びた部分１１０ａには、各種の外部デバイスが接続され

ている。外部デバイスについて後述する。

【００５０】

ＬＳＩ１０の内部に構成された内部回路１００には、さらにバスライン１１０の、外部への出入り口に介在するように、暗号化部１２０が備えられている。この暗号化部１２０は、暗号化回路１２１、バスインターフェース１２２、および乱数発生回路１２３から構成されている。

【００５１】

ＣＰＵ１０１には、発振器３０１からのクロック信号が入力され、ＣＰＵ１０１は、その発振器３０１から受けたクロック信号に同期して各種のプログラムを実行する。

【００５２】

また、暗号化回路１２１には、ＣＰＵ１０１に入力されるクロック信号よりも繰り返し周波数の高いクロック信号を発生するもう１つの発振器３０２からのクロック信号が入力され、暗号化回路１２１は、その発振器３０２からの繰り返し周波数の高いクロック信号に同期して暗号化処理が行なわれる。暗号化処理の詳細については後述する。

【００５３】

上記の２つの発振器３０１、３０２は、相互に同期したクロック信号を発生するものであり、したがって、共通の発振源で得られた高速クロックを分周して各クロック信号を生成するものであってもよい。

【００５４】

また、バスライン１１０の、外部に延びる部分１１０ａには、複数の外部デバイス、すなわち、この図１に示す例では、液晶表示装置（ＬＣＤ）２０１，キーボード（ＫＢ）２０２，読出専用メモリ（ＲＯＭ）２０３，フラッシュＲＯＭ２１１，ランダムアクセスメモリ（ＲＡＭ）２１２が接続されている。また、この図１には、この図１に示すＬＳＩ１０と同一の構成をもつもう１つのＬＳＩ等、内部回路１００と同様の暗号化機構を持つデバイス２１３も接続されており、さらに、ＣＰＵ１０１で動作するプログラムのデバッグのための逆暗号化回路２１４も接続されている。デバイス２１３および逆暗号化回路２１４は、それらの説

明のためにこの図１に一緒に示したものであるが、デバイス２１３は、ＬＳＩ１０と、そのＬＳＩ１０と同様な構成を持つデバイス２１３との間で暗号化通信を行なう場合に接続されるものであり、逆暗号化回路２１４はプログラムのデバッグのためのものであってデバッグ終了後は取り外されるものである。

【００５５】

ここで、ＬＣＤ２０１，ＫＢ２０２，および、この図１に示す実施形態においてはＲＯＭ２０３も、アドレスおよびデータの双方について暗号化を行なわない外部デバイスに属し、一方、フラッシュＲＯＭ２１１およびＲＡＭは、アドレスあるいはデータに関し暗号化を行なってアクセスする外部デバイスに属する。ここでは、フラッシュＲＯＭ２１１は、データのみ暗号化され、ＲＡＭは、アドレスとデータの双方について暗号化される。また、デバイス２１３もアドレスおよびデータの双方について暗号化されてＬＳＩ１０との間で暗号化通信が行なわれる。また、逆暗号化回路２１４が接続されるときは、この逆暗号化回路２１４は、本実施形態ではアドレスおよびデータの双方について暗号化を行なわないデバイスに属する。

【００５６】

ここで、バスライン１１０は、ＣＰＵ１０１に接続された部分（この部分のアドレス，データをそれぞれＡ１，Ｄ１と表記する）と、暗号化回路１２１とバスインターフェース１２２とに挟まれた部分（この部分のアドレス，データをそれぞれＡ２，Ｄ２と表記する）と、さらに、ＬＳＩ１０の外部に延びた部分１１０ａ（この部分のアドレス，データをそれぞれＡ３，Ｄ３と表記する）とに分かれている。

【００５７】

図２は、図１に示す処理装置のメモリマップを示す図である。

【００５８】

外部デバイスの１つであるフラッシュＲＯＭには、複数のアプリケーションプログラムが格納されており、内部デバイスの１つである内部メモリにはＯＳプログラムが格納されている。また、外部デバイスの１つであるＲＯＭには、この処理装置の装置構成情報、例えば接続されている外部デバイスの種類やメモリ容量

等が記録されている。

【００５９】

図３は、図１に示す処理装置に電源が投入されたときに実行される初期化プログラムのフローチャートである。この初期化プログラムは、ＯＳプログラムの一種として内部メモリ１０２に格納されており、電源投入時にＣＰＵ１０１で実行される。

【００６０】

図３に示す初期化プログラムでは、先ず外部デバイスの１つであるＲＯＭ２０３に格納された装置構成情報が読み出され（ステップａ１）、その情報に基づいて、図２に示すようなメモリマップが作成されるとともに、そのメモリマップの各エリアについて暗号化パターンが決定される（ステップａ２）。但し、アドレスもデータも暗号化しないということも、この暗号化パターンの１つとして含まれている。

【００６１】

この初期化プログラムでは、その後、その他の諸々の初期化処理が行なわれる（ステップａ３）。

【００６２】

図１に戻って説明を続行する。

【００６３】

ＣＰＵ１０１は、アドレスＡ１およびデータＤ１を用いて情報のリード，ライトを行なう。一方外部デバイスは、暗号化の必要なデバイスであるか暗号化は不要な（あるいは暗号化は禁止される）デバイスであるかに関わらず、アドレスＡ３およびデータＤ３を用いてアクセスされる。

【００６４】

ＣＰＵ１０１は、外部デバイスへのアクセスの前に、図２に示すメモリマップ上の、暗号化を行ないたいエリア（暗号化エリア）の領域情報と各暗号化エリアに対する暗号化パターンを、暗号化情報レジスタ１０３に書き込んでおく。

【００６５】

アドレスデコーダ１０４は、アドレスＡ１を入力するとともに暗号化情報レジ

スタ１０３から暗号化を行なうエリアを示す領域情報を受けとって、アクセス対象のデバイスに対し、チップセレクト信号ＣＳ０～ＳＣ６を出力するとともに、暗号化回路１２１に対し、どのデバイスがアクセス対象となっており暗号化が必要であるか否かを示す暗号化制御信号Ｃｒｐを出力する。

【００６６】

暗号化回路１２１は、アドレスデコーダから暗号化制御信号Ｃｒｐを受け取り、暗号化情報レジスタ１０３に記録されている暗号化パターンの情報を元に、アドレスＡ１，データＤ１について暗号化を行なう必要があるときにその暗号化エリアに応じた暗号化を行ない、アドレスＡ２，データＤ２を出力する。これらのアドレスＡ２，データＤ２は、バスインタフェース１２３を経由しアドレスＡ３，データＤ３としてＬＳＩ１０の外部に出力される。

【００６７】

ＣＰＵ１０１からバスインタフェース１２２には、外部デバイスをアクセス対象としているか否かを示す外部バスアクセス信号が伝達され、バスインタフェース１２２は、外部デバイスのアクセスが要求されているときは暗号化回路１２１から出力されたアドレスＡ２，データＤ２を外部のアドレスＡ３，データＤ３として外部に出力し、外部デバイスのアクセス要求がないときは、乱数発生回路１２３からの乱数を基に、ダミーのアドレス，データを生成して、外部のアドレスＡ３，データＤ３として出力する。このようにダミーのアドレス，データを出力することにより、不正な解析を一層困難にしている。

【００６８】

尚、ここでは、内部から外部へのアドレス，データの変換について述べたが、外部のフラッシュメモリ２１１やＲＡＭ２１２，ＲＯＭ２０３等から読み出されたデータＤ３については、バスインタフェース１２２はデータＤ２として内部に取り込み、そのデータが暗号化されたデータであるときは、暗号化回路１２１でその暗号化に対する復号化が行なわれ、暗号化前のデータＤ１として、ＣＰＵ１０１等に伝達される。

【００６９】

ここで、本実施形態においては暗号化パターンとして、アドレスもデータも暗

号化しないという暗号化パターンのほか、例えば、

（１）タイプ１

Ａ３＝Ａ１　ＸＯＲ　ｐ１

Ｄ３＝Ｄ１　ＸＯＲ　ｐ１

（２）タイプ２

Ａ３＝Ａ１

Ｄ３＝Ａ１＋Ｄ１＋ｐ１

（３）タイプ３

タイプ２の演算結果としてのデータについて、さらにそのデータの上位と下位を入れ替える

という暗号化パターンが採用される。

【００７０】

ここで、上記ｐ１は、例えば乱数等により得られた適当な定数であり、

Ａ　ＸＯＲ　Ｂは、ＡとＢの対応する各ビットごとの排他論理和演算を行なうことを意味し、Ａ＋Ｂは、Ａ，Ｂを数値とみたときの加算演算を意味している。

【００７１】

図３を参照して説明したように、電源投入時の初期化動作において、ＣＰＵ１０１は、外部デバイスの１つであるＲＯＭ２０３に格納された装置構成情報を読み出し、図２に示すようなメモリマップを作成するとともに、暗号化エリアについて暗号化パターンを決定するが、ここでは一例として、フラッシュＲＯＭ２１１については、アドレスについては暗号化は行なわずにデータについてのみ暗号化を行なう、例えば上記の（２）の暗号化パターンが採用され、ＲＡＭ２１２についてはアドレスおよびデータの双方について暗号化を行なう、例えば上記の（１）の暗号化パターンが採用される。

【００７２】

ここで、ＲＡＭ２１２については、上記（１）のタイプ１の暗号化パターンが採用されているため、例えばｐ１＝０ｘ５５５５（０ｘはそれに続く’５５５５’が１６進数であることを意味する）であるとすると、

Ａ３（０ｘ５４５５）

＝Ａ１（０ｘ０１００）　ＸＯＲ　ｐ１（０ｘ５５５５）

Ｄ３（０ｘ５４７６）

＝Ｄ１（０ｘ０１２３）　ＸＯＲ　ｐ１（０ｘ５５５５）

のように、アドレス及びデータとも、もとのアドレス，データとは全く異なる値となる。

【００７３】

また、フラッシュＲＯＭ２１１については、上記（２）タイプ２の暗号化パターンが採用されており、ｐ１＝０ｘ５５５５であるとすると、

Ａ３（０ｘ０１００）＝Ａ１（０ｘ０１００）

Ｄ３（０ｘ５７７８）

＝Ａ１（０ｘ０１００）＋Ｄ１（０ｘ０１２３）＋ｐ１（０ｘ５５５５）

のように、アドレスは変更されず、データについてはもとのデータとは全く異なる値となる。ここでは、データを暗号化するにあたり、アドレスＡ１の関数としているため、同一のデータＤ１であってもアドレスＡ１に応じて暗号化後のデータＤ３が異なることになり、不正な解析を一層困難にし、セキュリティの一層の向上が図られている。

【００７４】

尚、上記は暗号化パターンの計算上の例を挙げたものであり、アドレスを暗号化する場合、その暗号化対象のデバイスのアドレスエリアを越えて他のデバイスのアドレスエリアに移らないようにその暗号化のアルゴリズム上考慮されている。

【００７５】

また、例えば、同一のＲＡＭ２１２であっても、ＣＰＵ１０１で実行されるアプリケーションプログラムに応じてＲＡＭ２１２をアクセスするときの暗号化パターンを変更してもよい。そのようにメモリエリア（アクセスされる外部デバイス）に応じて暗号化パターンを選択するだけでなく、同一のメモリエリア（同一の外部デバイス）であっても、アプリケーションプログラムに応じても暗号化パターンを変更すると、バスライン１１０の、外部に延びた部分１１０ａに出力さ

れるアドレスやデータが一層複雑に暗号化されたものとなり、不正な解析がさらに困難となり、セキュリティの一層の向上が図られる。

【００７６】

ここで、ＣＰＵ１０１と暗号化回路１２１が仮に同一のクロックで動作していると、暗号化回路１２１では複雑な暗号化演算を行なうことができないことになる。例えばＣＰＵ１０１が１クロック毎に外部へアクセスを行なうとすると暗号化回路１２１は１クロック以内に暗号化処理を終える必要がある。例えば上述の（３）のタイプ３の暗号化処理の場合、（２）のタイプ２の暗号化を行なうのに１クロック分の時間を要し、さらに上位と下位を入れ替えるのに１クロック分の時間を要し、合計２クロック分の時間を要するものとすると、暗号化回路１２１で１クロック以内に暗号化処理を終える必要がある場合、この（３）のタイプ３の暗号化パターンは採用することができないことになる。

【００７７】

図１に示す実施形態の場合、ＣＰＵ１０１にクロックを供給する発振器３０１よりも高速なクロックを生成する発振器３０２を備え、暗号化回路１２１は発振器３０２から供給された高速なクロックに同期して動作するため、複数クロック必要とする、例えば上述の（３）のタイプ３の暗号化パターンや、さらに複雑な暗号化パターンを採用することができる。

【００７８】

例えばＣＰＵ１０１には、１０ＭＨｚのクロックが供給されており、暗号化回路１２１に１００ＭＨｚのクロックが供給されていると、暗号化回路では１０クロックを使って暗号化処理を行なうことができる。

【００７９】

また、図１に示す処理装置の内部回路１００はＬＳＩ１０の内部に作り込まれたものであり、そのＬＳＩ１０からは、暗号化回路１２１及びバスインタフェース１２２を経由して暗号化されたアドレスやデータが出力され、このままでは、このＬＳＩ１０を用いた製品を開発する際、ＣＰＵ１０１で実行されるプログラムのデバッグが極めて困難となる。そこで、図１に示す処理装置には、逆暗号化回路２１４が接続されている。

【００８０】

この逆暗号化回路２１４には、デバッグに先立って、ＣＰＵ１０１から、暗号化情報レジスタ１０３に書き込む内容と同様の内容の、暗号化パターン及び暗号化エリアの情報が書き込まれ、逆暗号化回路２１４は、その後のデバッグにおいて、前もって書き込まれた暗号化パターンや暗号化エリアの情報に基づいて、バスライン１１０の、外部に延びた部分１１０ａに出力された、暗号化されたアドレスやデータを復号化して、暗号化前のアドレスやデータを復元する。こうすることにより、その逆暗号化回路２１４により復元されたアドレスやデータを例えば計測器でもニタし、ＣＰＵ１０１で実行されるプログラムのデバッグを容易に行なうことができる。

【００８１】

この逆暗号化回路２１４は、このままにしておくと、不正な解析を困難にする目的でアドレスやデータを暗号化したことの意味を失うことになるため、別装置として構成しておいて、デバッグ終了後は取り外される。あるいは、そこに付けたまま完全に動作不能としてもよい。

【００８２】

また、図１には、ＬＳＩ１０と同様の暗号化機構をもつデバイス２１３が接続されている。このように、このＬＳＩ１０を複数組み合わせると、基板上でのＬＳＩ同士の暗号化通信を行なうことも可能となる。

【００８３】

図４は、本発明の処理装置の第２実施形態のブロック図である。

【００８４】

この図４に示す処理装置５は、ＬＳＩ５０の内部に組み込まれた内部回路５００とＬＳＩ５０の外部に外付けされた外部回路６００とから構成されている。ＬＳＩ５０は、本発明の集積回路の一実施形態にも相当する。

【００８５】

ＬＳＩ５０内に作り込まれた内部回路５００は、ＣＰＵ５０１、内部メモリ５０２、アドレスバススクランブル演算回路５０３、アドレスバススクランブルパターンメモリ５０４、データバススクランブル演算回路５０５、データバススク

ランブルパターンメモリ５０６、およびデコーダ回路５０７を有し、それらはバスライン５１０で相互に接続されている。このバスライン５１０はアドレスバス５１１とデータバス５１２とからなる。内部回路５００には、その他の内部デバイスも備えられているから、それらの図示及び説明は省略する。

【００８６】

ＬＳＩ１０内に作り込まれた内部回路５００の、図４に示す構成要素のうち、ＣＰＵ５０１および内部メモリ５０２を除く構成要素の複合、すなわち、アドレスバススクランブル演算回路５０３、アドレスバススクランブルパターンメモリ５０４、データバススクランブル演算回路５０５、データバススクランブルパターンメモリ５０６、およびデコーダ回路５０７の複合が、本発明にいう暗号化部の一例に相当する。

【００８７】

また、バスラインの、ＬＳＩ５０の外部に延びた部分には、外部回路６００を構成するＲＡＭ６０１とフラッシュＲＯＭ６０２が接続されている。

【００８８】

内部回路５００を構成する内部メモリ５０２にはＯＳプログラムが格納されており、また、外部回路５００を構成するフラッシュＲＯＭ６０２にはアプリケーションプログラムが格納されており、内部回路５００のＣＰＵ５０１ではそれら各種のプログラムが実行される。また、外部回路６００を構成するＲＡＭ６０１には、各種のデータが読み書き自在に格納される。

【００８９】

また、アドレスバススクランブル演算回路５０３およびデータバススクランブル演算回路５０５は、それぞれ、アドレスＡ０～１５およびデータＤ０～７をスクランブル（暗号化）する演算回路であり、アドレスバススクランブルパターンメモリ５０４およびデータバススクランブルパターンメモリ５０６には、それぞれアドレスバススクランブル演算回路５０３およびデータバススクランブル演算回路５０５におけるスクランブル演算において用いられるスクランブルパターンが格納されている。これらのアドレスバススクランブルパターンメモリ５０４およびデータバススクランブルパターンメモリ５０６は、不揮発性メモリ等により

構成されており、装置の電源が切断されても内容を保持することが可能であり、また、ＣＰＵ５０１により、スクランブルパターンの書き換えが可能である。

【００９０】

本実施形態では、アドレスバススクランブル演算回路５０３およびデータバススクランブル演算回路５０５のいずれにも、排他的論理和回路が採用されている。

【００９１】

図５は、排他的論理和回路を示す図である。

【００９２】

図５に示す排他的論理和回路（図４に示すアドレスバススクランブル演算回路５０３あるいはデータバススクランブル演算回路５０６）には、バスライン５１０を経由して入力ＩＮ（アドレスＡ０～１５あるいはデータＤ０～７）が入力されるとともに、アドレスバススクランブルパターンメモリ５０４あるいはデータバススクランブルパターンメモリ５０６から、スクランブルパターンＳＰ（ＳＰＡ０～１５あるいはＳＰＤ０～７）が入力され、出力ＯＵＴ（ＳＡ０～１５あるいはＳＰ０～７）として、

ＯＵＴ＝ＩＮ　ＸＯＲ　ＳＰ　　…（１）

但し、ＸＯＲは排他的論理和を表わす

が出力される。

【００９３】

ここで、スクランブルパターンＳＰを全ビットとも０にすることにより、スクランブルを禁止することができ、また一部のビットを０にすることにより、対応するビットのスクランブルを禁止することができる。例えば１６ビットのスクランブルパターンＳＰのうち下位４ビットを常に０にすると、下位４ビットについてはスクランブル（暗号化）が行なわれないことになる。

【００９４】

本実施形態におけるアドレスバススクランブル演算回路５０３およびデータバススクランブル演算回路５０５（以下、これらを総称するときは、単に、スクランブル演算回路と称する）には、上記（１）式に基づく演算を行なう排他的論理

和回路が採用されているが、以下に、スクランブル演算回路として採用することのできる各種の回路構成を例示しておく。

【００９５】

図６～図９は、スクランブル演算回路として採用することのできる各回路構成を示した図である。

【００９６】

図６に示すスクランブル演算回路には、加算回路が採用されており、ここでは

ＯＵＴ＝ＩＮ＋ＳＰ　　…（２）

の演算が行なわれる。

【００９７】

図７には、加算回路と排他的論理和回路が示されており、

ここでは、

ＯＵＴ＝（ＩＮ＋ＳＰ１）　ＸＯＲ　ＳＰ２　　…（３）

但し、ＳＰ１，ＳＰ２は、相互に異なる、あるいは同一の２つのスクランブルパターンである。

の演算が行なわれる。

【００９８】

また、図８には、排他的論理和回路とビット入換回路が示されており、ここでは、

ＯＵＴ＝（ＩＮ　ＸＯＲ　ＳＰ）$_{m}$　　…（４）

（排他的論理和演算を行なった後上位と下位のビットをｍビット分入れ換える）

の演算が行なわれる。

【００９９】

さらに、図９には、加算回路と排他的論理和回路が示されており、ここでは、

ＯＵＴ＝（ＩＮ（データ）＋ＩＮ（アドレス））　ＸＯＲ　ＳＰ　…（５）

但し、ＩＮ（データ）は、データバス上のデータ、ＩＮ（アドレス）はアドレスバス上のアドレスである。

の演算が行なわれる。但し、この（５）式に基づく演算は、データバススクラン

ブル演算回路５０５として採用可能なものであり、データをスクランブルするにあたりアドレスを用いると、不正な解析が一層困難な、極めて複雑なスクランブルが行なわれることになる。

【０１００】

図１０、図１１は、特定のビットのみスクランブルをかけるためのマスクパターンが付加されたスクランブル演算回路の各例を示す図である。

【０１０１】

図１０に示すスクランブル演算回路は、１つの反転回路と、２つの論理積回路と、１つの加算回路とからなり、この回路の場合、

ＯＵＴ＝（ＩＮ　ａｎｄ　Ｍ）＋ＳＰ＋（ＩＮ　ａｎｄ（ｎｏｔ　Ｍ））

…（６）

の演算が行なわれる。

【０１０２】

ここで、Ｍはマスクパターンを表わし、そのマスクパターンＭの中の、０が設定されたビットについては、スクランブルは行なわれない。例えば、１６ビットのうち下位４ビットのスクランブルを禁止するときは、マスクパターンＭとして０ｘＦＦＦ０が設定される。

【０１０３】

また、図１１に示すスクランブル演算回路は、１つの反転回路、２つの論理積回路、２つの加算回路、および１つの排他的論理和回路が図１１に示すように接続されたものであり、ここでは、

ＯＵＴ＝（（（ＩＮ　ａｎｄ　Ｍ）＋ＳＰ１）　ＸＯＲ　ＳＰ２）

＋（ＩＮ　ａｎｄ（ｎｏｔ　Ｍ））　…（７）

の演算が行なわれる。

【０１０４】

以上例示したように、スクランブル演算回路として様々な演算回路を採用することができる。

【０１０５】

図１２は、図４に示す第２実施形態の処理装置５におけるアドレスマップであ

る。

【０１０６】

図４には、代表的にＲＡＭは１つのみ示したが、実際にはワークＲＡＭとバックアップＲＡＭを備えており、ワークＲＡＭには、０ｘ００００００～０ｘ０ＦＦＦＦＦのアドレス領域（ワークＲＡＭ領域）が割り当てられており、バックアップＲＡＭには、装置の電源が切断された状態であっても電池等によりバックアップされ、その内容が保持されている。

【０１０７】

また、０ｘ２００００～０ｘ２ＦＦＦＦはＩＯ領域、０ｘ３００００～０ｘ３ＦＦＦＦはフラッシュＲＯＭ領域である。フラッシュＲＯＭには、各種のアプリケーションプログラムが格納されている。図４に示すアドレスバススクランブルパターンメモリ５０４およびデータバススクランブルパターンメモリ５０６は、ＩＯ領域（０ｘ２ＸＸＸＸの領域）に割り当てられている。

【０１０８】

ここで、図４に示すデコーダ回路は、アドレスＡ４～１９に基づいて、表１の真理値表に従って、データバススクランブルパターンメモリ５０６のライトイネーブル信号＊ＷＥＰＭＤおよびアドレスバススクランブルパターンメモリ５０４のライトイネーブル信号＊ＷＥＰＭＡを出力する。

【０１０９】

【表１】

A19	A18	A17	A16～5	A4	*WEPMD	*WEPMA
0	0	1	ALL 0	0	0	1
0	0	1	ALL 0	1	1	0
1	*	*	*	*	1	1
*	1	*	*	*	1	1
*	*	0	*	*	1	1
*	*	*	≠ALL0	*	1	1

【０１１０】

この表１は、０ｘ２０００Ｘのときにデータバススクランブルパターンメモリ５０６を書込み可能状態（＊ＷＥＰＭＤ＝０）とし、０ｘ２００１Ｘのときにア

ドレスバススクランブルパターンメモリ５０４を書込み可能状態（＊ＷＥＰＭＡ＝０）とすることを意味している。

【０１１１】

図１３は、データバススクランブルパターンメモリ５０６の構成を示す図である。このデータバススクランブルパターンメモリ５０６は、２つのデコーダ（デコーダ１とデコーダ２）と、４つのデータラッチ（データラッチ０～３）で構成されている。データラッチ０～３は、それぞれ、ワークＲＡＭ，バックアップＲＡＭ，ＩＯ，フラッシュＲＯＭのデータをスクランブルするための各スクランブルパターンの格納領域であり、後に示す表４にあるように、それぞれ、アドレス０ｘ２０００，０ｘ２００１，０ｘ２００２，０ｘ２００３が割り当てられている。

【０１１２】

デコーダ１は、各データラッチ０～３に格納されている各スクランブルパターンを選択的に出力させるための各アウトプットイネーブル信号＊ＯＥ０～＊ＯＥ３を生成する回路であり、表２の真理値表に示す論理構成となっている。

【０１１３】

【表２】

A19	A18	A17	A16	*OE0	*OE1	*OE2	*OE3
0	0	0	0	0	1	1	1
0	0	0	1	1	0	1	1
0	0	1	0	1	1	0	1
0	0	1	1	1	1	1	0
1	*	*	*	1	1	1	1
*	1	*	*	1	1	1	1

【０１１４】

また、デコーダ２は、各データラッチ０～３に新たなスクランブルパターンを書き込むための各ライトイネーブル信号＊ＷＥ０～＊ＷＥ３を生成する回路であり、表３の真理値表に示す論理構成となっている。

【０１１５】

【表３】

*WEPMD	A0	A1	*WE0	*WE1	*WE2	*WE3
1	*	*	1	1	1	1
0	0	0	0	1	1	1
0	0	1	1	0	1	1
0	1	0	1	1	0	1
0	1	1	1	1	1	0

【０１１６】

データラッチ０～３は、各々に対応するライトイネーブル信号＊ＷＥ０～３が０になると、そのタイミングでデータバス５１２に出力されているＤ０～７のデータを記憶し、また、各々に対応するアウトプットイネーブル信号＊ＯＥ０～３が０になると記憶しているスクランブルパターンをＳＰＤ０～７のデータとして出力する。ここで、アウトプットイネーブル信号＊ＯＥ０～３の全てが１の場合は、ＳＰＤ０～７のデータは全てのビットが０となる。

【０１１７】

ここで、本実施形態では、データバス５１２上のデータは８ビット幅（Ｄ０～７）であるのに対し、アドレスバス５１１は、スクランブルとは無関係の拡張ビットＳＡ１６～１９を除き１６ビット幅（Ａ０～Ａ１５）である。図１３にはデータバススクランブルパターンメモリ５０６の構成を示したが、アドレスバススクランブルパターンメモリ５０４は、データと比べてアドレスのビット幅が広いことに伴い、図１３に示すデータラッチ０～３がそれぞれ２バイト構成になり、各データラッチを選択するためのアドレスがＡ０～３の４ビット（図１３に示すデータバススクランブルパターンメモリ５０６の場合はデータラッチを選択するためのアドレスはＡ０～１の２ビットである）となることを除き、構成としては図１３に示すデータバススクランブルパターンメモリ５０６の構成と同様であり、アドレスバススクランブルパターンメモリ５０４の図示及びこれ以上の説明は省略する。

【０１１８】

本実施形態では、データバススクランブルパターンメモリ５０６の各データラッチ０～３およびアドレスバススクランブルパターンメモリ５０４の各データラ

ッチには、表４に示すアドレスが割り当てられており、各アドレスにそれらの各アドレスに対応するスクランブルの各対象領域についてスクランブルを実行するためのスクランブルパターンが書き込まれ、ＣＰＵ５０１から出力されるアドレス情報（Ａ０～１９）に従って、各データラッチに書き込まれているスクランブルパターンがスクランブル演算回路に向けて出力される。

【０１１９】

【表４】

アドレス	対象メモリ	対象ラッチ名	対象領域
２００００	データバススクランブルパターンメモリ	データラッチ０	ワーク RAM
２０００１		データラッチ１	バックアップ RAM
２０００２		データラッチ２	IO
２０００３		データラッチ３	フラッシュ ROM
２０００８	アドレスバススクランブルパターンメモリ	データラッチ０　下位バイト	ワーク RAM
２０００９		データラッチ０　上位バイト	
２０００Ａ		データラッチ１　下位バイト	バックアップ RAM
２０００Ｂ		データラッチ１　上位バイト	
２０００Ｃ		データラッチ２　下位バイト	IO
２０００Ｄ		データラッチ２　上位バイト	
２０００Ｅ		データラッチ３　下位バイト	フラッシュ ROM
２０００Ｆ		データラッチ３　上位バイト	

【０１２０】

表５は、本実施形態におけるパターンメモリの設定例を示す表である。

【０１２１】

【表５】

領域	アドレス範囲	アドレスバススクランブルパターン	データバススクランブルパターン
ワークＲＡＭ	０ｘ００００００～０ｘ０ＦＦＦＦ	０ｘ３ＣＢ０	０ｘ２５
バックアップＲＡＭ	０ｘ１００００～０ｘ１ＦＦＦＦ	０ｘ２Ａ５０	０ｘ６Ｅ
ＩＯ	０ｘ２００００～０ｘ２ＦＦＦＦ	０ｘ００００	０ｘ００
フラッシュＲＯＭ	０ｘ３００００～０ｘ３ＦＦＦＦ	０ｘ４１Ｄ９	０ｘ２Ｂ

【０１２２】

本実施形態で採用されているＲＡＭは、下位４ビットについて連続したアドレスでアクセスした場合に高速なアクセスが可能な素子であり、したがって表５に示すように、ＲＡＭのアドレスバススクランブルパターンの下位４ビットは０（スクランブルを行なわないことを意味する）に設定されており、ＣＰＵからの連続したメモリアクセスの場合の高速なアクセス速度を保証している。

【０１２３】

また、ＩＯ空間はスクランブルを禁止するために、全てのビットが０に設定されている。

【０１２４】

図１４は、図４に示す処理装置における、電源投入時およびリセット時に動作するプログラムの一部を示した図である。

【０１２５】

ここでは、１６ビットの乱数ＲＡと８ビットの乱数ＲＤが生成され（ステップｂ１，ｂ２）、１６ビットの乱数ＲＡと０ｘＦＦＦ０との論理積演算結果がアドレス０ｘ２０００８～９に書き込まれ（（ステップｂ３）、８ビットの乱数ＲＤがアドレス０ｘ２００００に書き込まれる。表４に示すようにアドレス０ｘ２０００８～９はワークＲＡＭ用のアドレスバススクランブルパターンの格納領域、アドレス０ｘ２００００はワークＲＡＭ用のデータバススクランブルパターンの格納領域である。

【０１２６】

すなわち、ここでは、電源投入あるいはリセットのたびにワークＲＡＭのスクランブルパターンが変更されることになり、このことも、外部からの不正な解析を一層困難にするのに役立っている。

【０１２７】

尚、バックアップＲＡＭやフラッシュＲＯＭについては、そこに格納されたデータやプログラムの一貫性が必要なため、あらかじめ定められたスクランブルパターンがそのまま保持され、電源の再投入やリセットが行なわれても、スクランブルパターンは変更されない。

【０１２８】

フラッシュＲＯＭについては、工場での書込み時にはスクランブルをかけないでおくことも可能である。その場合、出荷後の最初の電源投入時に、以下の手順によりスクランブルがかけられる。

【０１２９】

図１５は、電源投入時に動作するプログラムの、フラッシュＲＯＭのスクランブルの部分を示すフローチャートである。

【０１３０】

ここでは、先ず、フラッシュＲＯＭの内容がスクランブルされたものであるか否かを示すスクランブル有無フラグがチェックされる。このスクランブル有無フラグはバックアップＲＡＭの所定の番地に格納されており、工場での書込み時に、このスクランブル有無フラグは‘無’に設定される。

【０１３１】

このスクランブル有無フラグの確認は、フラッシュＲＯＭの内容が既にスクランブル済であるか否かの判定のためであり、スクランブル有無フラグを設定する代わりに、フラッシュＲＯＭに対応するスクランブルパターンを読み出し、そのスクランブルパターンの全ビットが０であることをもって、未だスクランブルが行なわれていないものと判定してもよい。

【０１３２】

ステップｃ１でスクランブル有無フラグがスクランブル‘無’に設定されていると判定されると、ステップｃ２に進み、フラッシュＲＯＭの内容がＲＡＭにコピーされる。このフラッシュＲＯＭの一部には、以下の処理を行なうためのプログラムが書込まれている。

【０１３３】

次いで、ＲＡＭにコピーされたプログラムのうち、以下の処理を行なうためのプログラムに制御が移され、フラッシュＲＯＭが消去され（ステップｃ４）、１６ビットの乱数ＲＡと８ビットの乱数ＲＤが生成され（ステップｃ５，ｃ６）、１６ビットの乱数ＲＡがフラッシュＲＯＭのアドレススクランブルパターンとしてアドレス０ｘ２０００Ｅ～Ｆに書き込まれるとともに８ビットの乱数ＲＤがフラッシュＲＯＭのデータスクランブルパターンとしてアドレス０ｘ２０００３に

書き込まれる（表４を参照；ステップｃ７，ｃ８）。

【０１３４】

次に、ステップｃ２でＲＡＭにコピーされたプログラムが、アドレス０ｘ２０００Ｅ～Ｆおよびアドレス０ｘ２０００３に書き込まれたアドレススクランブルパターンおよびデータスクランブルパターンでスクランブルされてフラッシュＲＯＭに書き戻され（ステップｃ９）、フラッシュＲＯＭスクランブル有無フラグが‘有’に変更される（ステップｃ１０）。

【０１３５】

こうすることにより、フラッシュＲＯＭの内容が最初の電源投入時にスクランブルされることになる。

【０１３６】

また、工場出荷時には特定のスクランブルパターンでスクランブルしておいて、最初の電源投入時に別のスクランブルパターンでスクランブルし直すようにしてもよい。この場合、工場出荷時にスクランブルされた内容を元に戻すための逆スクランブルパターン（ここではスクランブルパターンを参照することによって元に戻すことができるためスクランブルパターンそのものである）は、スクランブルパターンメモリに書き込んでおくこともでき、フラッシュＲＯＭ内に書き込んでおいてもよい。フラッシュＲＯＭ内に書き込んでおくと、工場出荷時点ではスクランブルパターンメモリについて電池等でバックアップしておく必要がないという利点がある。

【０１３７】

図１６は、フラッシュＲＯＭに、あらかじめスクランブルされたプログラムが書き込まれており、かつそのスクランブルを元に戻すのに必要なスクランブルパターンがフラッシュＲＯＭ内に格納されて出荷されたときの、電源投入時に動作するプログラムの、フラッシュＲＯＭのスクランブルの部分を示すフローチャートである。このプログラムは、図１５に示すプログラムに代えて実行されるプログラムである。

【０１３８】

ステップｄ１では、工場出荷前のスクランブルを除き、フラッシュＲＯＭが既

にスクランブルされたか否かを示すスクランブル有無フラグが参照される。工場出荷前のスクランブルを除き、未だ一度もスクランブルされていないときはステップｄ２～ｄ１２の各ステップが実行される。

【０１３９】

ステップｄ２，ｄ３では、フラッシュＲＯＭに格納されている、アドレスバススクランブルパターンＳＰＡ０およびデータバススクランブルパターンＳＰＤ０がそれぞれアドレス０ｘ２０００Ｅ～Ｆおよびアドレス０ｘ２０００３に書き込まれる（表４参照）。

【０１４０】

次にステップｄ４において、フラッシュＲＯＭの内容がスクランブルパターンＳＰＡ０，ＳＰＤ０に基づいてスクランブルされる前の状態に戻されてＲＡＭにコピーされる。

【０１４１】

その後の各ステップｄ５～ｄ１２は、図１５の各ステップｃ３～ｃ１０とそれぞれ同一であり、重複説明は省略する。

【０１４２】

この図１６に示すプログラムの実行により、フラッシュＲＯＭの内容が、最初の電源投入時に新たに生成した乱数ＲＡ，ＲＢをアドレススクランブルパターン，データスクランブルパターンとして再度スクランブルされ、その後はそのスクランブルされた状態が保持される。

【０１４３】

ここで、上記の例は、スクランブルパターンがフラッシュＲＯＭに書き込まれた例であるが、例えばフラッシュＲＯＭの内容を、工場出荷前に、個々の製品毎に別々のスクランブルパターンでスクランブルしておき、そのスクランブルを解除するための逆スクランブルパターンを特定の暗号処理により暗号化して、バックアップＲＡＭ等、フラッシュＲＯＭとは別の領域に書き込んでおいてもよい。そのときはその暗号化されたスクランブルパターンを暗号化前のスクランブルパターンに戻すための復号処理の手続も、ＬＳＩ５０の内部のいずれかの領域に埋め込まれる。

【０１４４】

上記の暗号処理としては、例えば公開鍵暗号方式（例えばＲＡＳ等）を用いることができる。すなわち、公開鍵（Ｋｐｂ）で暗号化された逆スクランブルパターンをフラッシュＲＯＭあるいは他のメモリに書き込んでおき、その暗号化されたスクランブルパターンをＬＳＩ５０内のいずれかの領域に埋め込んでおいた秘密鍵（Ｋｐｖ）で復号する。このようなシステムの場合、同一仕様のＬＳＩ５０を複数の会社で使用した場合であっても、各会社に公開鍵のみを渡し、秘密鍵は伏せておくことにおり、会社間のセキュリティが確保できる。

【０１４５】

図１７は、フラッシュＲＯＭについて工場出荷前にスクランブルしておき、そのスクランブルを解除するためのスクランブルパターンを公開鍵Ｋｐｂにより暗号化してバックアップＲＡＭに格納し、その状態で出荷された後の電源投入時に動作するプログラムの、フラッシュＲＯＭのスクランブルの部分を示すフローチャートである。

【０１４６】

ステップｅ２，ｅ３では、バックアップＲＡＭより、公開鍵で暗号化された状態のアドレスバススクランブルパターンＫｐｂ（ＳＰＡ０）が読み出され、ＬＳＩの内部に埋め込まれた秘密鍵Ｋｐｖにより復号化されて平文のアドレスバススクランブルパターンＳＰＡ０が取り出される。

【０１４７】

また、ステップｅ４，ｅ５では、バックアップＲＡＭより、公開鍵で暗号化された状態のデータバススクランブルパターンＫｐｂ（ＳＰＤ０）が読み出され、ＬＳＩの内部に埋め込まれた秘密鍵Ｋｐｖにより復号化されて平文のデータバススクランブルパターンが取り出される。

【０１４８】

ステップｅ６，ｅ７では、上記のようにして得られた平文のアドレスバススクランブルパターンＳＰＡ０および平文のデータバススクランブルパターンＳＰＤ０が、それぞれ、アドレス０ｘ２０００Ｅ～Ｆおよびアドレス０ｘ２０００３に書き込まれる（表４参照）。

【０１４９】

その後の各ステップｅ８～ｅ１６は、図１６の各ステップｄ４～ｄ１２とそれぞれ同一であり、重複説明は省略する。

【０１５０】

図１８は、本発明の処理装置の第３実施形態のブロック図である。

【０１５１】

図４に示す第２実施形態からの相違点について説明する。

【０１５２】

この第３実施形態では、外部回路６００に、図４の第２実施形態と同様のＲＡＭ６０１およびフラッシュＲＯＭ６０２が備えられているほか、さらに通信制御回路６０３が備えられている。

【０１５３】

この通信制御回路６０３は通信回路網８００を介して鍵管理センター７００と接続されている。フラッシュＲＯＭ６０２には、工場出荷前にスクランブルされた状態のプログラムが格納されており、最初の電源投入時に、鍵管理センター７００から、通信回路網８００を経由して、暗復号化されたスクランブルパターンを受け取るように構成されている。

【０１５４】

図１９は、図１８に示す処理装置における電源投入時に実行されるプログラムの、フラッシュＲＯＭのスクランブルに関する部分のフローチャートである。

【０１５５】

図１９のステップｆ１は、図１７のステップｅ１と同じである。

【０１５６】

ステップｆ２では鍵管理センターへの接続が行なわれ、ステップｆ３では、鍵管理センターから、公開鍵Ｋｐｂで暗号化された形式のアドレスバススクランブルパターンｋｐｂ（ＳＰＡ０）およびデータバススクランブルパターンＫｐｂ（ＳＰＤ０）がダウンロードされる。

【０１５７】

ステップｆ４，ｆ５では、ＬＳＩに埋め込まれた秘密鍵Ｋｐｖにより、暗号化

された状態のアドレスバススクランブルパターンＫｐｂ（ＳＰＡ０）および暗号化された状態のデータバススクランブルパターンＫｐｂ（ＳＰＤ０）がそれぞれ復号化されて、平文のアドレスバススクランブルパターンＳＰＡ０およびデータバススクランブルパターンＳＰＤ０が取り出される。

【０１５８】

それ以降の各ステップｆ６～ｆ１６は図１７の各ステップｅ６～ｅ１６とそれぞれ同一であり、重複説明は省略する。

【０１５９】

このように、通信により鍵管理センター等の外部からスクランブルパターンの入手を可能とすることにより、システムの柔軟性が確保される。

【０１６０】

図２０は、本発明の処理装置の第４実施形態のブロック図である。

【０１６１】

図４に示す第２実施形態との相違点について説明する。

【０１６２】

図２０に示す第４実施形態では、外部回路６００に、図４の第２実施形態の場合と同様のＲＡＭ６０１およびラッシュＲＯＭ６０２が備えられているほか、タンパ検出スイッチ６０４が備えられており、さらにバックアップ用電池６０５が明示的に示されている。

【０１６３】

アドレスバススクランブルパターンメモリ５０４およびデータバススクランブルパターンメモリ５０６は、電源が切断された状態においてもバックアップ用電池６０５からの電力によりその内容が消去されないようバックアップされている。

【０１６４】

ここで、この処理装置５が不正に開けられた場合にタンパ検出スイッチ６０４が働き、バックアップ用電池６０５からの電力供給経路が遮断され、アドレスバススクランブルパターンメモリ５０４およびデータバススクランブルパターンメモリ５０６に格納されていたアドレスバススクランブルパターンおよびデータバ

スクランブルパターンが消去され、この処理装置の動作が不能となる。こうすることにより、不正な解析がさらに確実に防止される。

【０１６５】

尚、上記の各実施形態では、１つのＬＳＩの内部に作り込まれた回路を内部回路、そのＬＳＩの外部に外付けされたデバイスの集合を外部回路と称しているが、内部回路は必ずしも１つのＬＳＩに搭載されたものである必要はなく、例えば複数のＬＳＩに分散して搭載されてそれら複数のＬＳＩが１つの集積回路パッケージ内にパッケージされ、あるいは、それら複数のＬＳＩが一体にモールドされたものである場合に、それら複数のＬＳＩに分散して搭載された回路全体を内部回路と称してもよい。

【０１６６】

以下、本発明の各種態様を付記する。

【０１６７】

（付記１）　プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、前記ＣＰＵと前記内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

前記バスラインの外部に延びた部分に外付けされた、各所定の作用を成す１つ以上の外部デバイスを含む外部回路を備え、

前記内部回路が、前記バスラインの、外部への出入口に介在し、該バスライン上のアドレスおよびデータを、前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部を含むものであることを特徴とする処理装置。

【０１６８】

（付記２）　前記暗号化部で採用される暗号化パターンには、アドレスおよびデータの双方とも暗号化しないことを１つの暗号化パターンとして含むものであることを特徴とする付記１記載の処理装置。

【０１６９】

（付記３）　前記外部回路が複数の外部デバイスを含むものであり、

前記暗号化部は、前記複数の外部デバイスそれぞれに応じた暗号化パターンで

暗号化するものであることを特徴とする付記１記載の処理装置。

【０１７０】

（付記４）　前記暗号化部は、前記外部回路がアクセスされていないタイミングで、前記バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることを特徴とする付記１記載の処理装置。

【０１７１】

（付記５）　前記ＣＰＵは、クロックの供給を受け供給されたクロックに同期してプログラムを実行するものであるとともに、前記暗号化部も、クロックの供給を受け供給されたクロックに同期して暗号化を行なうものであって、

前記暗号化部に、前記ＣＰＵに供給されるクロックよりも高速なクロックを供給するクロック供給部を備えたことを特徴とする付記１記載の処理装置。

【０１７２】

（付記６）　前記外部回路の構成を認識し、その構成に応じて、前記暗号化部における暗号化パターンを決定する暗号化パターン決定手段を有することを特徴とする付記１記載の処理装置。

【０１７３】

（付記７）　前記暗号化部は、前記バスライン上のアドレスおよびデータを、前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じるとともに前記ＣＰＵで実行されるアプリケーションプログラムにも応じた暗号化パターンで暗号化するものであることを特徴とする付記１記載の処理装置。

【０１７４】

（付記８）　前記バスラインの、外部に延びた部分に接続され、該バスライン上の暗号化されたアドレスおよびデータを暗号化前のアドレスおよびデータに戻す逆暗号化部を備えたことを特徴とする付記１記載の処理装置。

【０１７５】

（付記９）　前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することを特徴

とする付記１記載の処理装置。

【０１７６】

（付記１０）　前記暗号化部は、前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることを特徴とする付記１記載の処理装置。

【０１７７】

（付記１１）　プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、前記ＣＰＵと前記内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

前記バスラインの、外部に延びた部分に外付けされた、情報を記憶するメモリを含む外部回路を備え、

前記内部回路が、前記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする処理装置。

【０１７８】

（付記１２）　前記所定の初期化動作が、最初の電源投入時の初期化動作であることを特徴とする付記１記載の処理装置。

【０１７９】

（付記１３）　前記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることを特徴とする付記１１記載の処理装置。

【０１８０】

（付記１４）　前記メモリに記憶された情報のうちの少なくとも一部の情報が、前記所定の初期化動作を実行する以前において既に暗号化されたものであって、

前記情報書換手段は、該少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであることを特徴とする付記１１記載の処理装置。

【０１８１】

（付記１５）　前記少なくとも一部の情報を暗号化前の情報に戻すための復号化情報が前記メモリに記憶されてなるものであって、

前記情報書換手段は、該少なくとも一部の情報を、該復号化情報を用いて一旦暗号化前の情報に戻すものであることを特徴とする付記１４記載の処理装置。

【０１８２】

（付記１６）　前記少なくとも一部の情報が公開鍵により暗号化されたものであるとともに、この処理装置は秘密鍵が埋め込まれてなるものであって、

前記情報書換手段は、該少なくとも一部の情報を該秘密鍵を用いて一旦暗号化前の情報に戻すものであることを特徴とする付記１４記載の処理装置。

【０１８３】

（付記１７）　前記少なくとも一部の情報を暗号化前の情報に戻すための、暗号化された形式の復号化情報を外部より取得する情報取得部を備え、

前記情報書換手段は、前記情報取得部で取得された、暗号化された形式の復号化情報を復号化して平文の復号化情報を取り出しこの平文の復号化情報を用いて該少なくとも一部の情報を一旦暗号化前の情報に戻すものであることを特徴とする付記１４記載の処理装置。

【０１８４】

（付記１８）　前記内部回路が前記暗号化部で採用される暗号化パターンを保持してなるものであって、

タンパ検出を行なうタンパ検出部を備えるとともに、

前記タンパ検出部によるタンパ検出を受けて前記内部回路内に保持されていた暗号化パターンを破壊する情報破壊手段を備えたことを特徴とする付記１又は１１記載の処理装置。

【０１８５】

（付記１９）　プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、前記ＣＰＵと前記内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、各所定の作用を成す１つ以上の外部デバイスが外付けされる、アドレスおよびデータを伝達するバスラインと、該バスラインの

、外部への出入口に介在し、該バスライン上のアドレスおよびデータを、該バスラインの、外部に延びた部分に外付けされた１つ以上の外部デバイス全体に割り当てられた空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部とが搭載されてなることを特徴とする集積回路。

【０１８６】

（付記２０）　前記暗号化部で採用される暗号化パターンには、アドレスおよびデータの双方とも暗号化しないことを１つの暗号化パターンとして含むものであることを特徴とする付記１８記載の集積回路。

【０１８７】

（付記２１）　前記バスラインの、外部に延びた部分に、複数の外部デバイスが外付けされた場合に、前記暗号化部は、前記複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることを特徴とする付記１９記載の集積回路。

【０１８８】

（付記２２）　前記暗号化部は、前記外部回路がアクセスされていないタイミングで、前記バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることを特徴とする付記１９記載の集積回路。

【０１８９】

（付記２３）　前記ＣＰＵは、クロックの供給を受け供給されたクロックに同期してプログラムを実行するものであるとともに、前記暗号化部も、クロックの供給を受け供給されたクロックに同期して暗号化を行なうものであって、

前記暗号化部は、前記ＣＰＵが動作するクロックよりも高速なクロックで動作するものであることを特徴とする付記１９記載の集積回路。

【０１９０】

（付記２４）　前記外部回路の構成を認識し、その構成に応じて、前記暗号化部における暗号化パターンを決定する暗号化パターン決定手段を有することを特徴とする付記１９記載の集積回路。

【０１９１】

（付記２５）　前記暗号化部は、前記バスラインの、アドレスおよびデータ

を前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じるとともに前記ＣＰＵで実行されるアプリケーションプログラムにも応じた暗号化パターンで暗号化するものであることを特徴とする付記１９記載の集積回路。

【０１９２】

（付記２６）　前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することを特徴とする付記１９記載の集積回路。

【０１９３】

（付記２７）　前記暗号化部は、前記１つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることを特徴とする付記１９記載の集積回路。

【０１９４】

（付記２８）　プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、前記ＣＰＵと前記内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、情報を記憶するメモリが外付けされる、アドレスおよびデータを伝達するバスラインとを備えるとともに、

前記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする集積回路。

【０１９５】

（付記２９）　前記所定の初期化動作が、最初の電源投入時の初期化動作であることを特徴とする付記２８記載の集積回路。

【０１９６】

（付記３０）　前記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることを特徴とする付記２８記載の集積回路。

【０１９７】

（付記３１）　前記メモリに記憶された情報のうちの少なくとも一部の情報が、前記所定の初期化動作を実行する以前において既に暗号化されたものであって、

前記情報書換手段は、該少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであることを特徴とする付記２８記載の集積回路。

【０１９８】

（付記３２）　前記少なくとも一部の情報を暗号化前の情報に戻すための復号化情報が前記メモリに記憶されてなるものであって、

前記情報書換手段は、該少なくとも一部の情報を、該復号化情報を用いて一旦暗号化前の情報に戻すものであることを特徴とする付記３１記載の集積回路。

【０１９９】

（付記３３）　前記少なくとも一部の情報が公開鍵により暗号化されたものであるとともに、この集積回路は秘密鍵が埋め込まれてなるものであって、

前記情報書換手段は、該少なくとも一部の情報を該秘密鍵を用いて一旦暗号化前の情報に戻すものであることを特徴とする付記３１記載の集積回路。

【０２００】

（付記３４）　前記少なくとも一部の情報を暗号化前の情報に戻すための、暗号化された形式の暗号化情報を外部より取得する情報取得部を備え、

前記情報書換手段は、前記情報取得部で取得された、暗号化された形式の復号化情報を復号化して平文の復号化情報を取り出しこの平文の復号化情報を用いて該少なくとも一部の情報を一旦暗号化前の情報に戻すものであることを特徴とする付記３１記載の集積回路。

【０２０１】

【発明の効果】

以上、説明したように、本発明によれば、外付けされたデバイスにプログラムやデータ等を記憶させても、それらを第３者による不正なリバースエンジニアリング等の行為から守る事ができ、従来よりも高いセキュリティを保つことができ

る。

【図面の簡単な説明】

【図１】

本発明の処理装置の第１実施形態を示すブロック図である。

【図２】

図１に示す処理装置のメモリマップを示す図である。

【図３】

図１に示す処理装置に電源が投入されたときに実行される初期化プログラムのフローチャートである。

【図４】

本発明の処理装置の第２実施形態のブロック図である。

【図５】

排他的論理和回路を示す図である。

【図６】

スクランブル演算回路として採用することのできる回路構成を示した図である。

【図７】

スクランブル演算回路として採用することのできる回路構成を示した図である。

【図８】

スクランブル演算回路として採用することのできる回路構成を示した図である。

【図９】

スクランブル演算回路として採用することのできる回路構成を示した図である。

【図１０】

特定のビットのみスクランブルをかけるためのマスクパターンが付加されたスクランブル演算回路の一例を示す図である。

【図１１】

特定のビットのみスクランブルをかけるためのマスクパターンが付加されたスクランブル演算回路のもう１つの例を示す図である。

【図１２】

図４に示す第２実施形態の処理装置におけるアドレスマップである。

【図１３】

データバススクランブルパターンメモリの構成を示す図である。

【図１４】

図４に示す処理装置における、電源投入時およびリセット時に動作するプログラムの一部を示した図である。

【図１５】

電源投入時に動作するプログラムの、フラッシュＲＯＭのスクランブルの部分を示すフローチャートである。

【図１６】

フラッシュＲＯＭにあらかじめスクランブルされたプログラムが書き込まれており、かつそのスクランブルを元に戻すのに必要な逆スクランブルパターンがフラッシュＲＯＭ内に格納されて出荷されたときの、電源投入時に動作するプログラムの、フラッシュＲＯＭのスクランブルの部分を示すフローチャートである。

【図１７】

フラッシュＲＯＭについて工場出荷前にスクランブルしておき、そのスクランブルを解除するための逆スクランブルパターンを公開鍵Ｋｐｂにより暗号化してバックアップＲＡＭに格納し、その状態で出荷された後の電源投入時に動作するプログラムの、フラッシュＲＯＭのスクランブルの部分を示すフローチャートである。

【図１８】

本発明の処理装置の第３実施形態のブロック図である。

【図１９】

図１８に示す処理装置における電源投入時に実行されるプログラムの、フラッシュＲＯＭのスクランブルに関する部分のフローチャートである。

【図２０】

本発明の処理装置の第４実施形態のブロック図である。

【符号の説明】

１，５　処理装置

１０，５０　ＬＳＩ

１００　内部回路

１０１　中央処理装置（ＣＰＵ）

１０２　内部メモリ

１０３　暗号化情報レジスタ

１０４　アドレスデコーダ

１０５　周辺回路

１２０　暗号化部

１２１　暗号化回路

１２２　バスインターフェース

１２３　乱数発生回路

２００　外部回路

２０１　液晶表示装置（ＬＣＤ）

２０２　キーボード（ＫＢ）

２０３　読出専用メモリ（ＲＯＭ）

２１１　フラッシュＲＯＭ

２１２　ランダムアクセスメモリ（ＲＡＭ）

２１３　デバイス

２１４　逆暗号化回路

３０１，３０２　発振器

５００　内部回路

５０１　ＣＰＵ

５０２　内部メモリ

５０３　アドレスバススクランブル演算回路

５０４　アドレスバススクランブルパターンメモリ

５０５　データバススクランブル演算回路

５０６　データバススクランブルパターンメモリ

５０７　デコーダ回路

５１０　バスライン

５１１　アドレスバス

５１２　データバス

６００　外部回路

６０１　ＲＡＭ

６０２　フラッシュＲＯＭ

６０３　通信制御回路

６０４　タンパ検出スイッチ

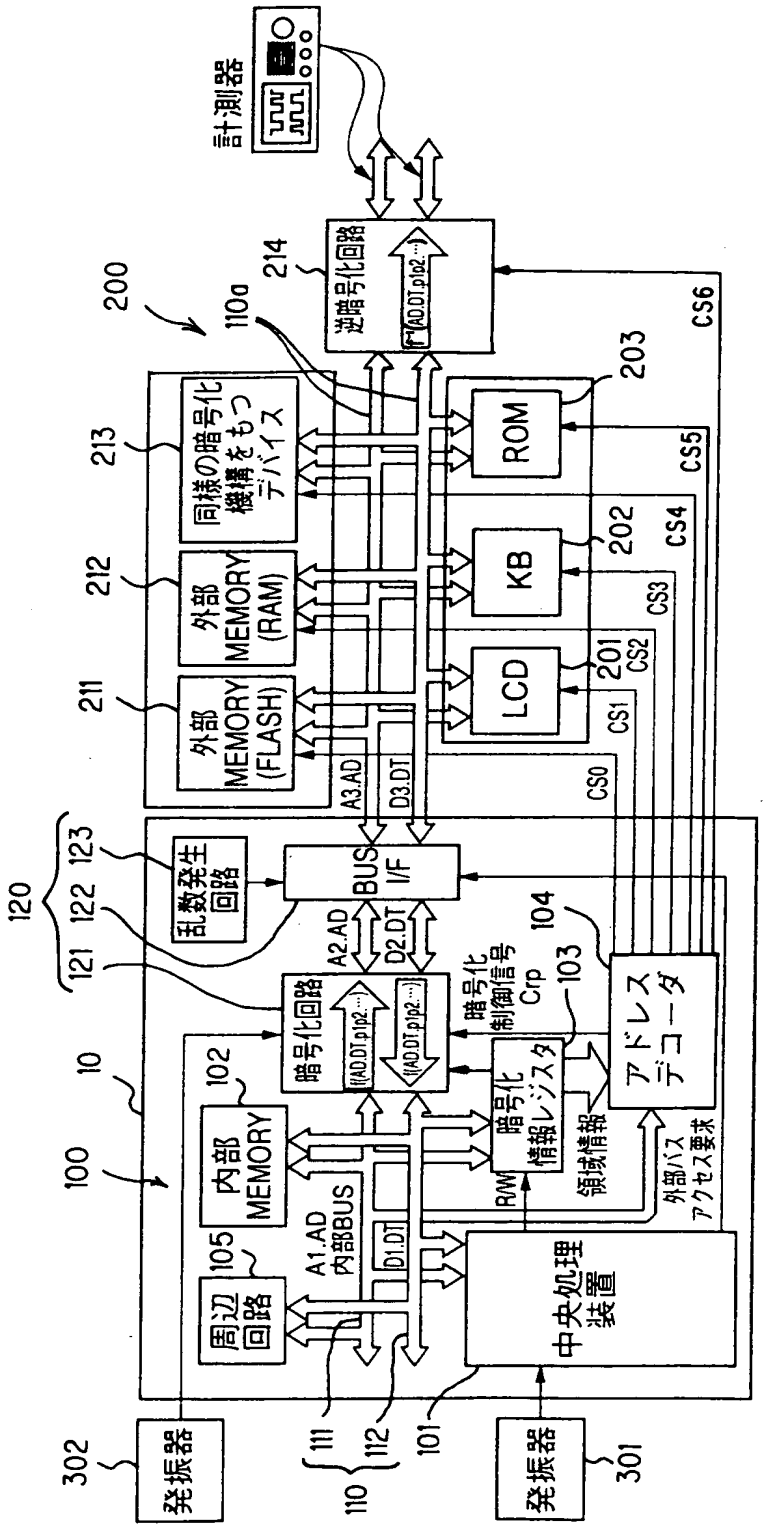
６０５　バックアップ用電池

７００　鍵管理センター

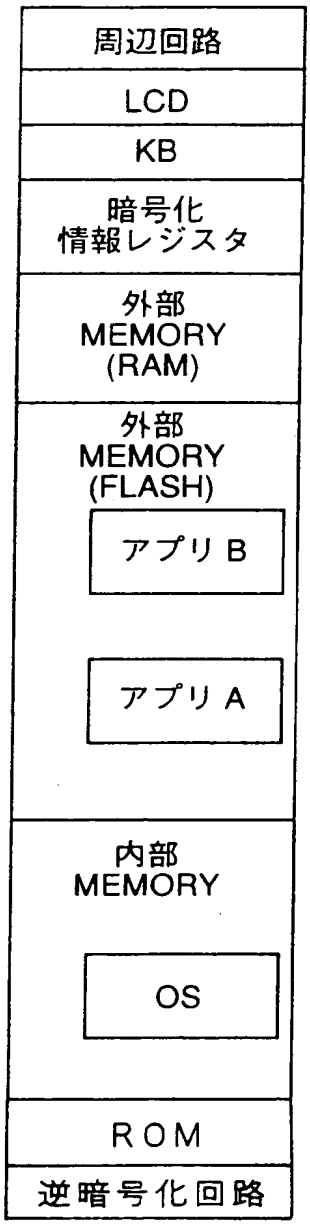
８００　通信回路網

【書類名】　　図面

【図１】

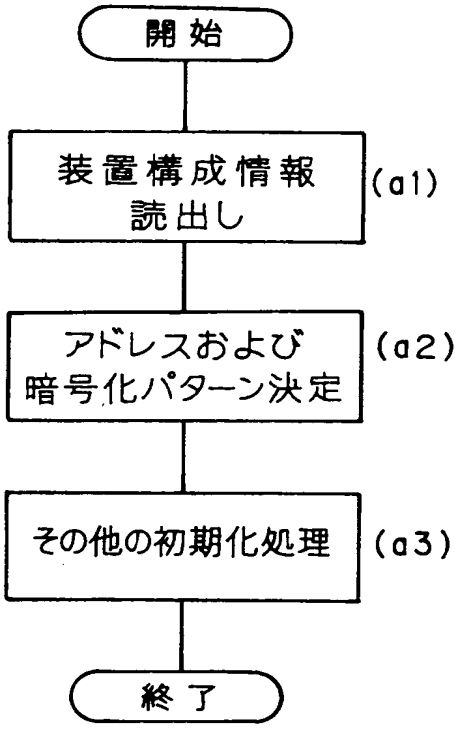

計測器
逆暗号化回路
(AD.DT.p1p2...)
214
200
110a
CS6
203
ROM
CS5
202
KB
CS4
CS3
201
LCD
CS2
CS1
CS0
213
同様の暗号化機構をもつデバイス
212
外部MEMORY(RAM)
211
外部MEMORY(FLASH)
A3.AD
D3.DT
120
123
乱数発生回路
122
121
BUS I/F
A2.AD
D2.DT
104
暗号化制御信号 Crp
103
暗号化回路
(AD.DT.p1p2...)
(AD.DT.p1p2...)
アドレスデコーダ
102
10
100
内部MEMORY
暗号化情報レジスタ
R/W
領域情報
外部バスアクセス要求
A1.AD
内部BUS
D1.DT
105
周辺回路
中央処理装置
302
発振器
111
112
110
101
発振器
301

【図２】

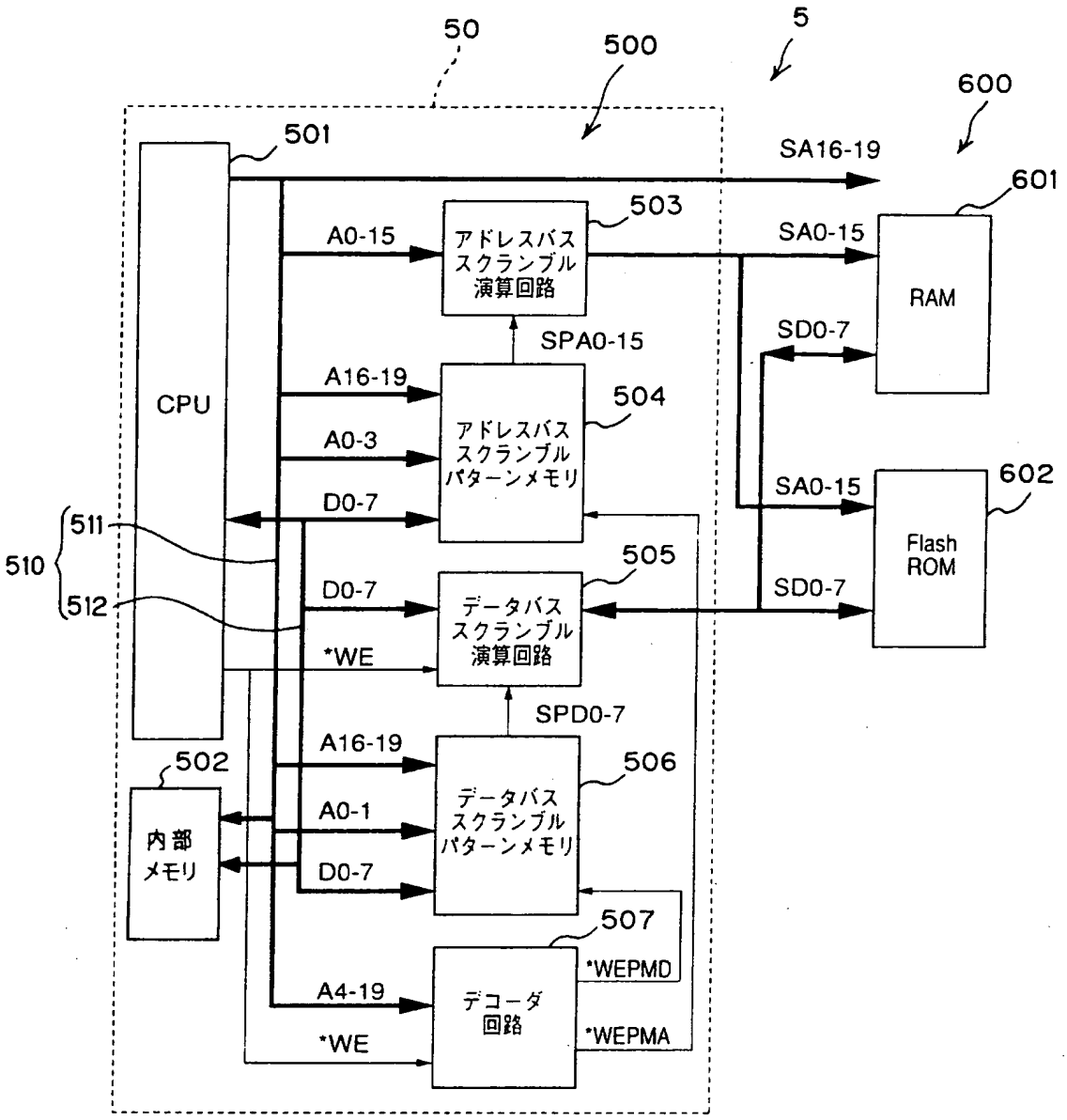


出証特２０００－３０８４６１９

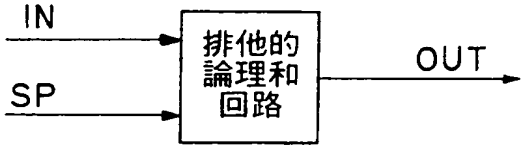
【図３】



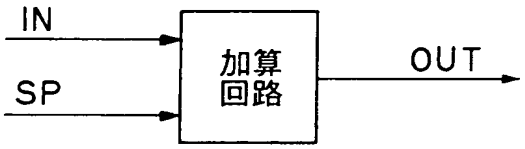
【図４】


50
500
5
600
501
SA16-19
601
503
A0-15
アドレスバス
スクランブル
演算回路
SA0-15
RAM
SD0-7
SPA0-15
CPU
A16-19
504
アドレスバス
スクランブル
パターンメモリ
A0-3
D0-7
SA0-15
602
511
510
512
505
D0-7
データバス
スクランブル
演算回路
Flash
ROM
SD0-7
*WE
SPD0-7
A16-19
502
506
内部
メモリ
A0-1
データバス
スクランブル
パターンメモリ
D0-7
507
*WEPMD
A4-19
デコーダ
回路
*WEPMA
*WE

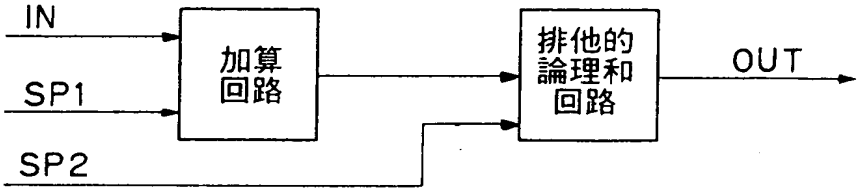
【図５】


IN
SP
排他的
論理和
回路
OUT

【図６】


IN
SP
加算
回路
OUT

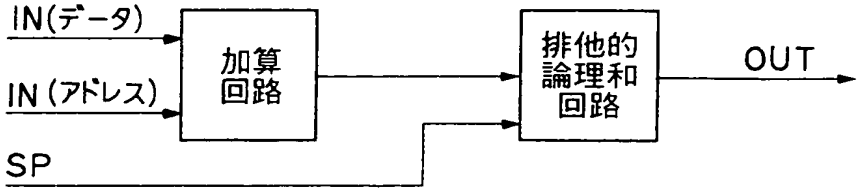
【図７】


IN
SP1
SP2
加算
回路
排他的
論理和
回路
OUT

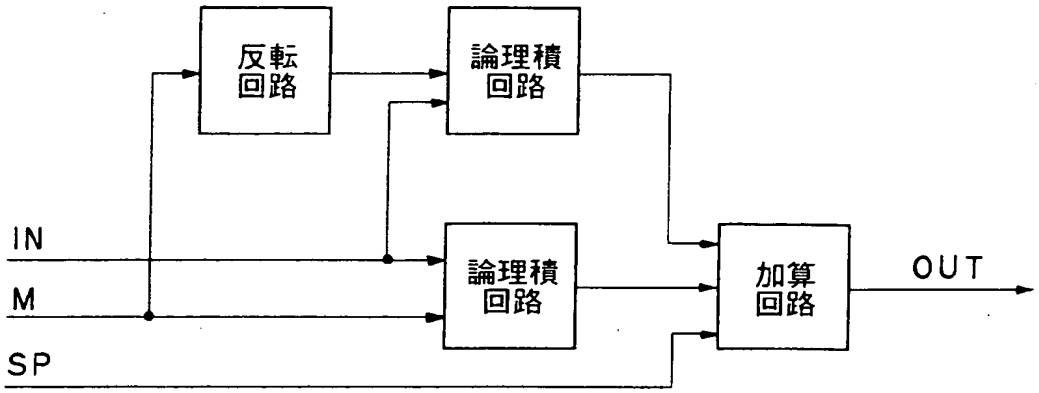
【図８】


IN
SP
排他的
論理和
回路
ビット
入換
回路
OUT

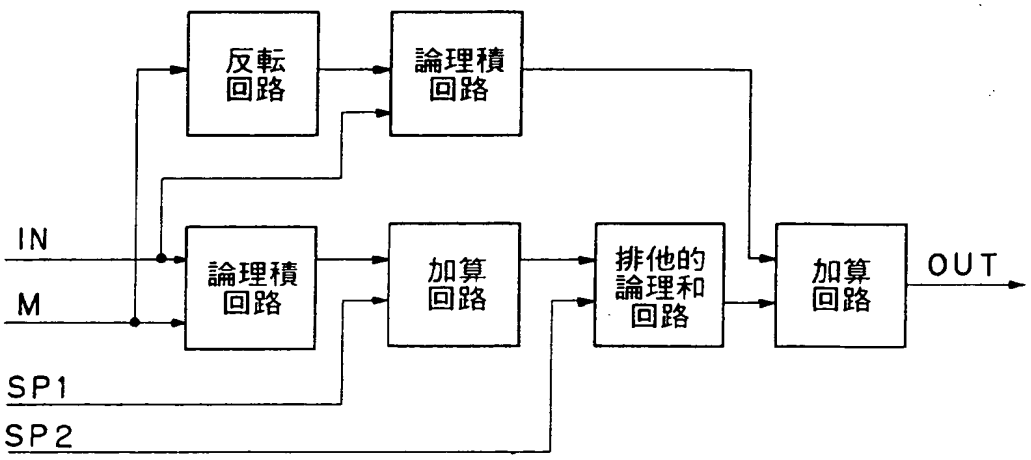
【図９】


IN(データ)
IN(アドレス)
SP
加算
回路
排他的
論理和
回路
OUT

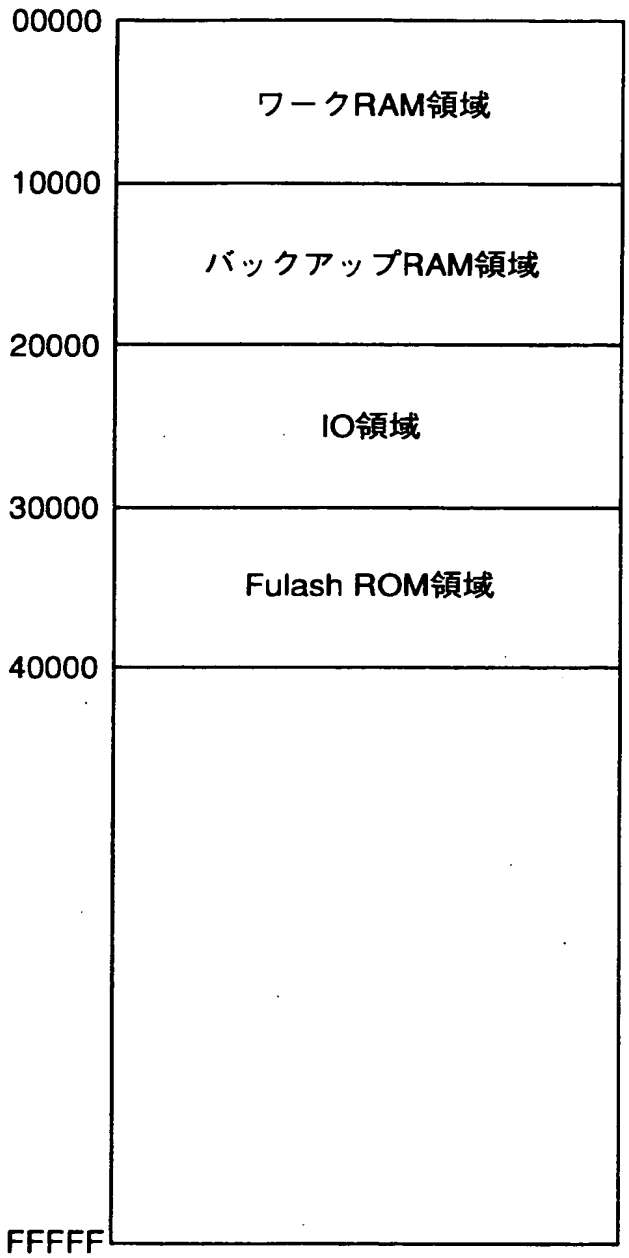
【図１０】


反転
回路
論理積
回路
IN
M
SP
論理積
回路
加算
回路
OUT

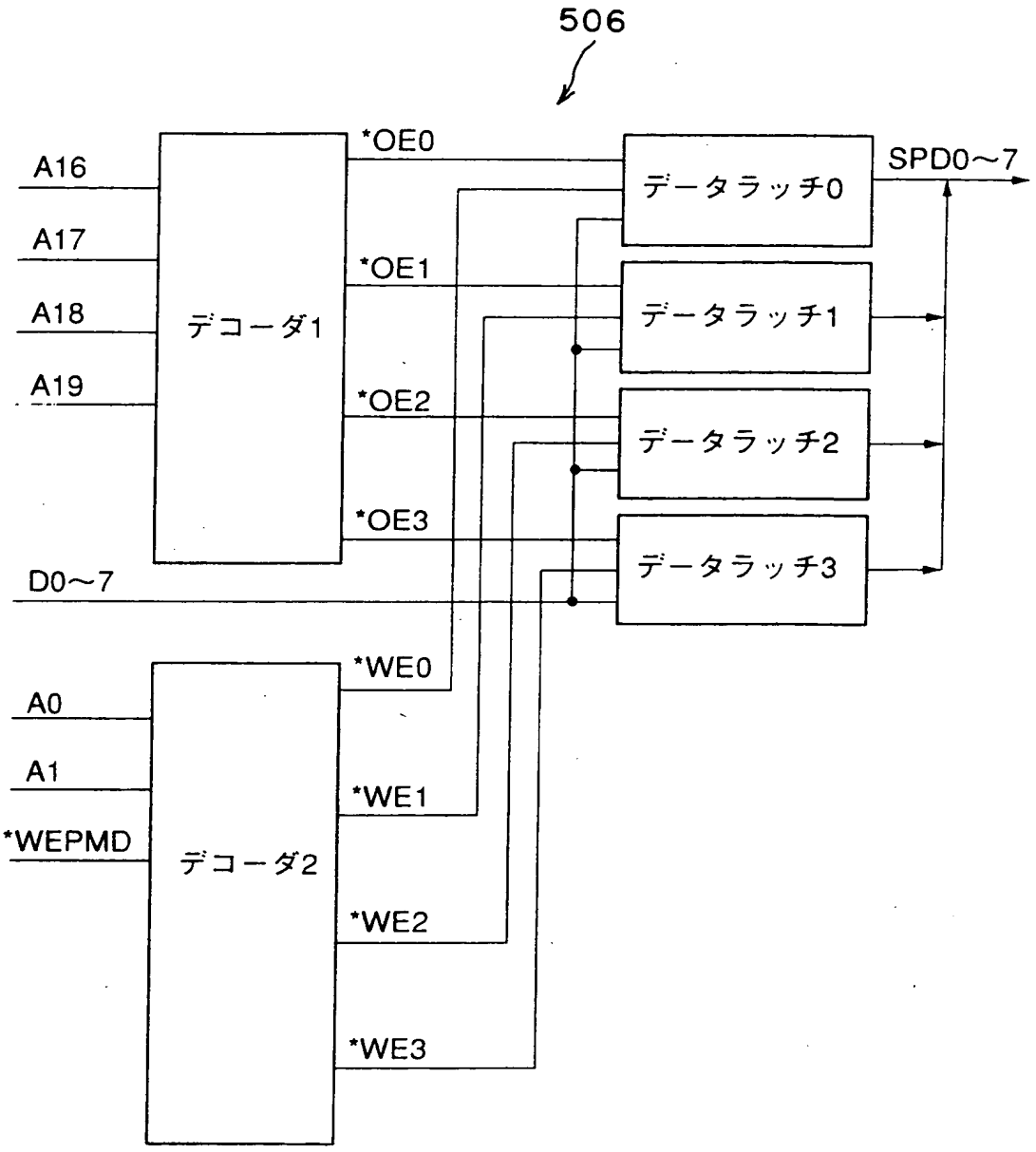
【図１１】


反転
回路
論理積
回路
IN
M
論理積
回路
加算
回路
排他的
論理和
回路
加算
回路
OUT
SP1
SP2

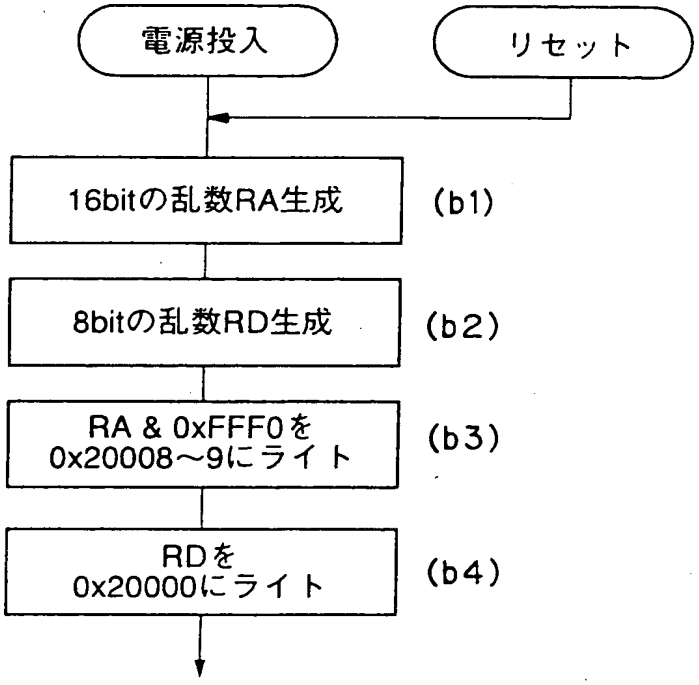
【図１２】


00000
ワークRAM領域
10000
バックアップRAM領域
20000
IO領域
30000
Fulash ROM領域
40000
FFFFF

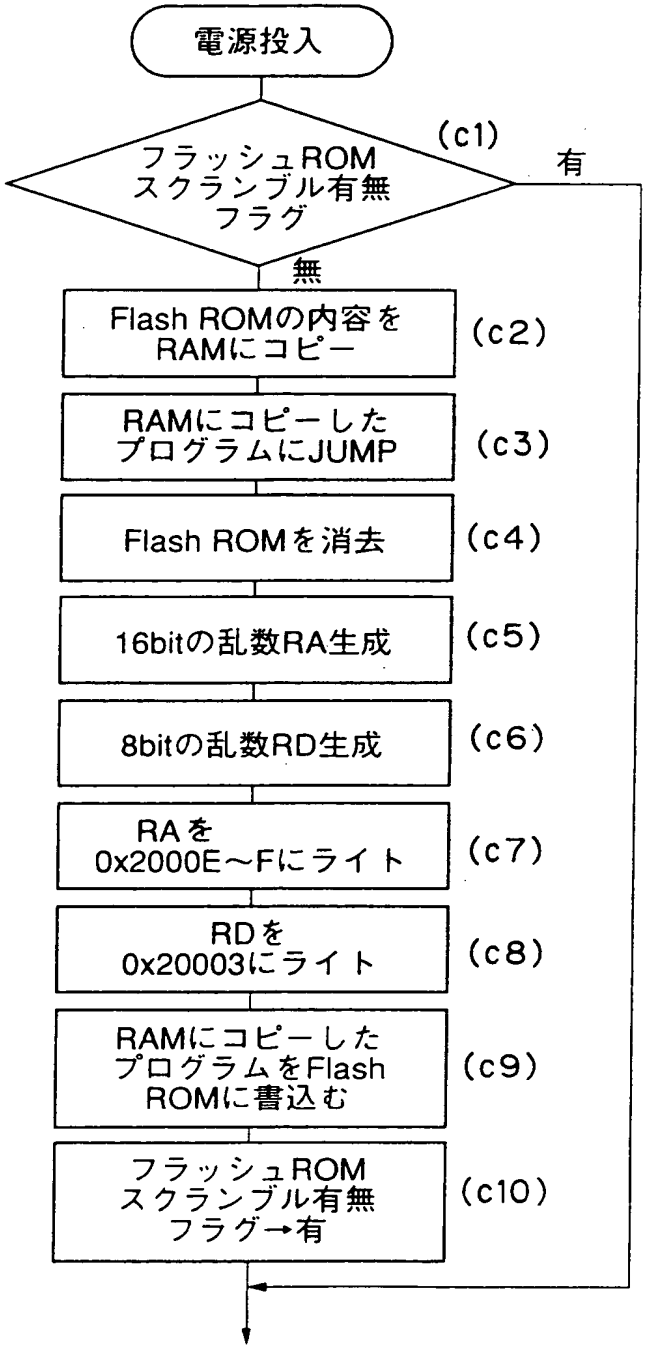
【図１３】


506
A16
A17
A18
A19
デコーダ1
*OE0
*OE1
*OE2
*OE3
D0～7
データラッチ0
データラッチ1
データラッチ2
データラッチ3
SPD0～7
A0
A1
*WEPMD
デコーダ2
*WE0
*WE1
*WE2
*WE3

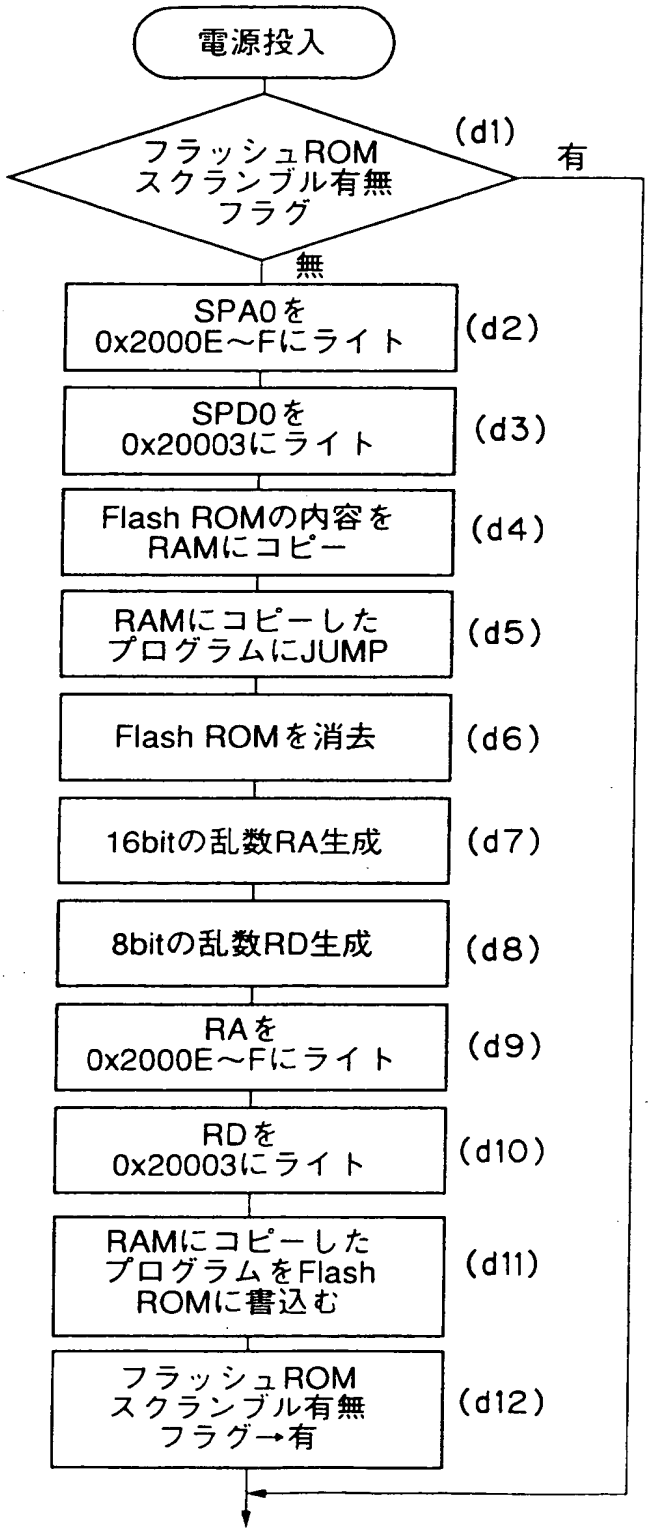
【図１４】


電源投入
リセット
16bitの乱数RA生成
(b1)
8bitの乱数RD生成
(b2)
RA & 0xFFF0を
0x20008～9にライト
(b3)
RDを
0x20000にライト
(b4)

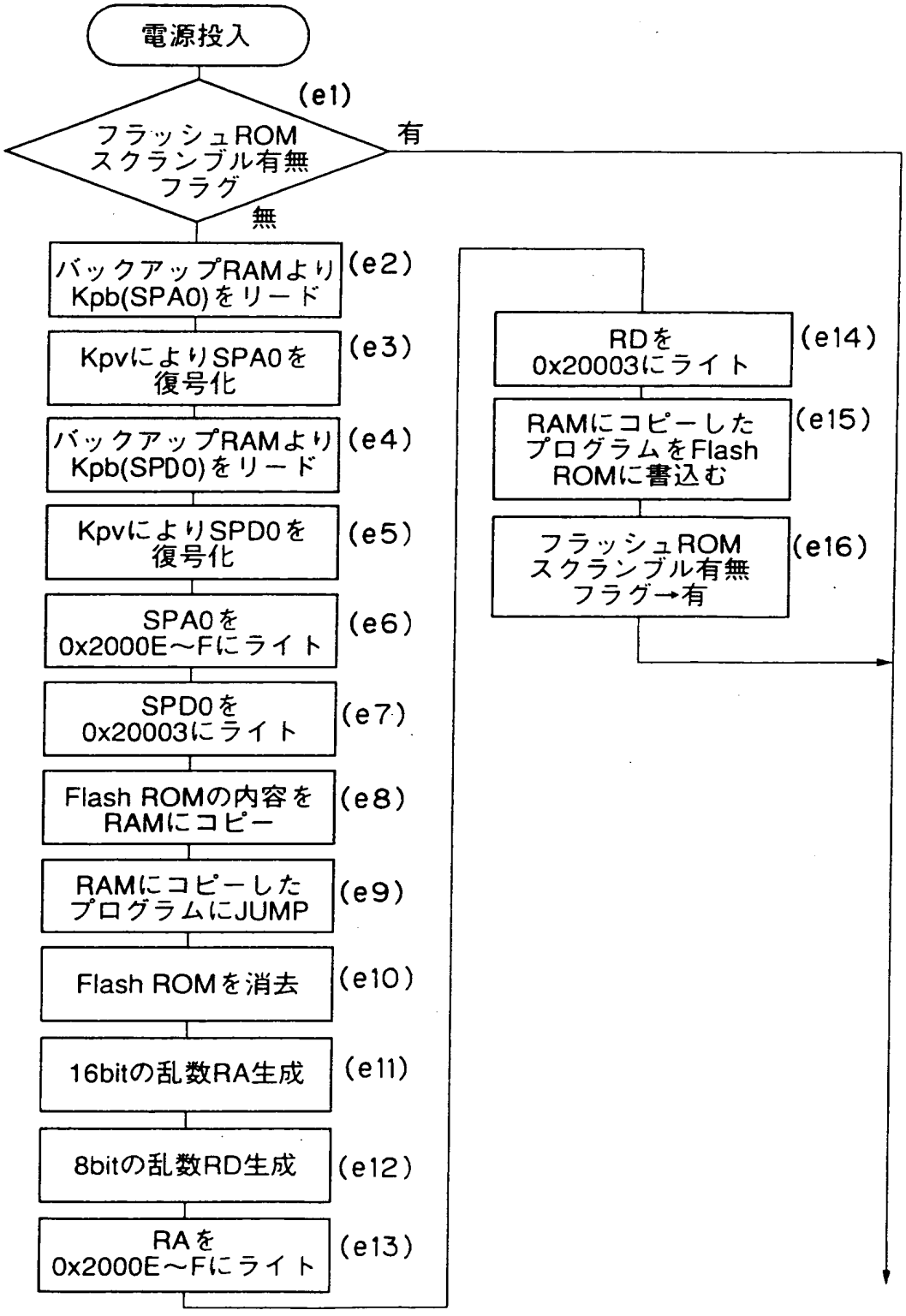
【図１５】


電源投入
フラッシュROM
スクランブル有無
フラグ
(c1)
有
無
Flash ROMの内容を
RAMにコピー
(c2)
RAMにコピーした
プログラムにJUMP
(c3)
Flash ROMを消去
(c4)
16bitの乱数RA生成
(c5)
8bitの乱数RD生成
(c6)
RAを
0x2000E～Fにライト
(c7)
RDを
0x20003にライト
(c8)
RAMにコピーした
プログラムをFlash
ROMに書込む
(c9)
フラッシュROM
スクランブル有無
フラグ→有
(c10)

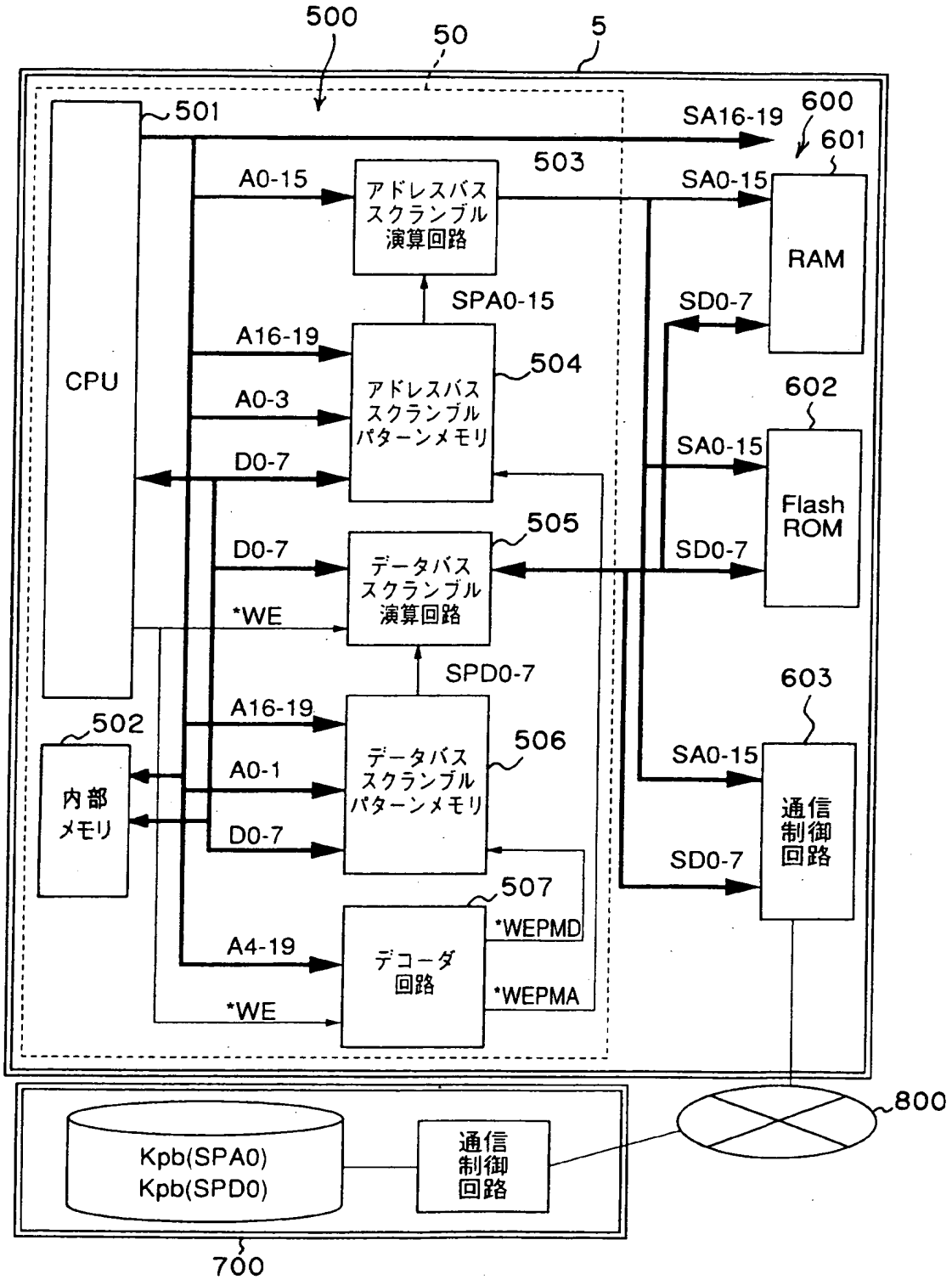
【図１６】


電源投入
フラッシュROM
スクランブル有無
フラグ
(d1)
有
無
SPA0を
0x2000E～Fにライト
(d2)
SPD0を
0x20003にライト
(d3)
Flash ROMの内容を
RAMにコピー
(d4)
RAMにコピーした
プログラムにJUMP
(d5)
Flash ROMを消去
(d6)
16bitの乱数RA生成
(d7)
8bitの乱数RD生成
(d8)
RAを
0x2000E～Fにライト
(d9)
RDを
0x20003にライト
(d10)
RAMにコピーした
プログラムをFlash
ROMに書込む
(d11)
フラッシュROM
スクランブル有無
フラグ→有
(d12)

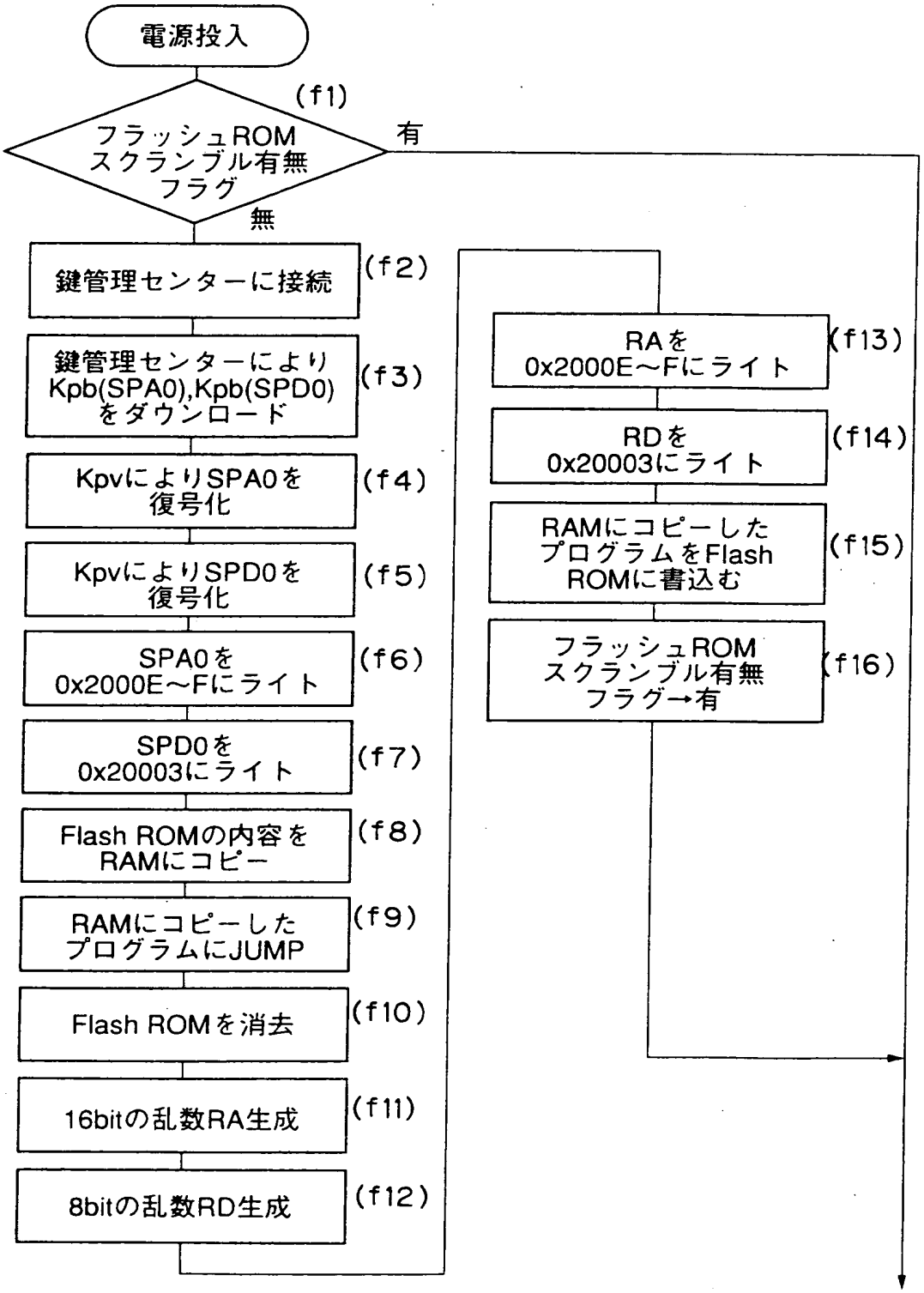
【図１７】


電源投入
(e1)
フラッシュROM
スクランブル有無
フラグ
有
無
バックアップRAMより
Kpb(SPA0)をリード
(e2)
KpvによりSPA0を
復号化
(e3)
バックアップRAMより
Kpb(SPD0)をリード
(e4)
KpvによりSPD0を
復号化
(e5)
SPA0を
0x2000E～Fにライト
(e6)
SPD0を
0x20003にライト
(e7)
Flash ROMの内容を
RAMにコピー
(e8)
RAMにコピーした
プログラムにJUMP
(e9)
Flash ROMを消去
(e10)
16bitの乱数RA生成
(e11)
8bitの乱数RD生成
(e12)
RAを
0x2000E～Fにライト
(e13)
RDを
0x20003にライト
(e14)
RAMにコピーした
プログラムをFlash
ROMに書込む
(e15)
フラッシュROM
スクランブル有無
フラグ→有
(e16)

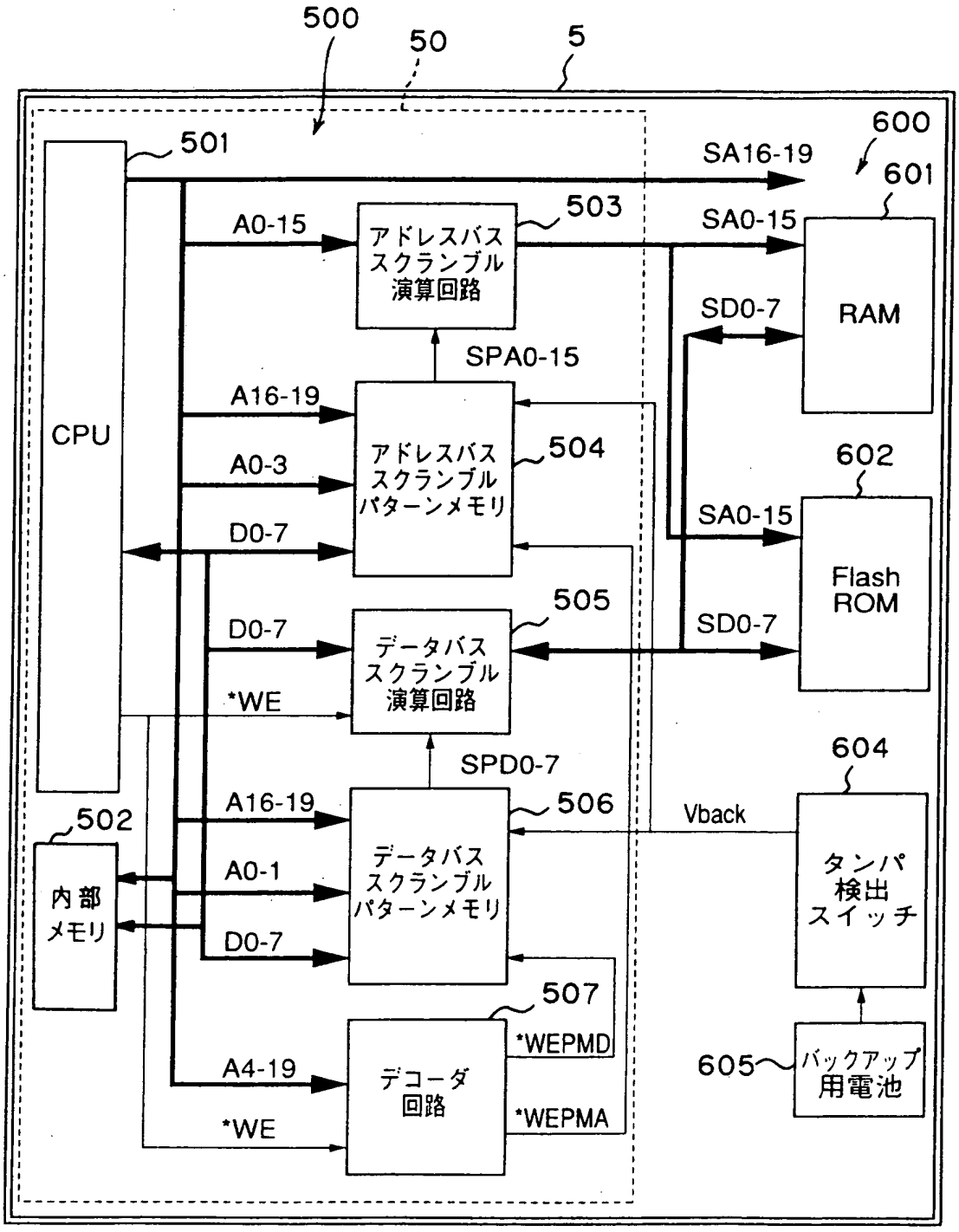
【図１８】


500
50
5
501
SA16-19
600
601
503
A0-15
アドレスバス
スクランブル
演算回路
SA0-15
RAM
SPA0-15
SD0-7
A16-19
504
CPU
A0-3
アドレスバス
スクランブル
パターンメモリ
602
SA0-15
D0-7
Flash
ROM
505
D0-7
データバス
スクランブル
演算回路
SD0-7
*WE
SPD0-7
603
502
A16-19
506
SA0-15
内部
メモリ
A0-1
データバス
スクランブル
パターンメモリ
通信
制御
回路
D0-7
SD0-7
507
*WEPMD
A4-19
デコーダ
回路
*WEPMA
*WE
800
Kpb(SPA0)
Kpb(SPD0)
通信
制御
回路
700

【図１９】


電源投入
(f1)
フラッシュROM
スクランブル有無
フラグ
有
無
鍵管理センターに接続
(f2)
鍵管理センターにより
Kpb(SPA0),Kpb(SPD0)
をダウンロード
(f3)
KpvによりSPA0を
復号化
(f4)
KpvによりSPD0を
復号化
(f5)
SPA0を
0x2000E～Fにライト
(f6)
SPD0を
0x20003にライト
(f7)
Flash ROMの内容を
RAMにコピー
(f8)
RAMにコピーした
プログラムにJUMP
(f9)
Flash ROMを消去
(f10)
16bitの乱数RA生成
(f11)
8bitの乱数RD生成
(f12)
RAを
0x2000E～Fにライト
(f13)
RDを
0x20003にライト
(f14)
RAMにコピーした
プログラムをFlash
ROMに書込む
(f15)
フラッシュROM
スクランブル有無
フラグ→有
(f16)

【図２０】


500
50
5
501
SA16-19
600
601
A0-15
503
アドレスバス
スクランブル
演算回路
SA0-15
RAM
SD0-7
SPA0-15
CPU
A16-19
A0-3
D0-7
アドレスバス
スクランブル
パターンメモリ
504
602
SA0-15
Flash
ROM
SD0-7
D0-7
505
データバス
スクランブル
演算回路
*WE
SPD0-7
604
A16-19
506
Vback
502
内部
メモリ
A0-1
D0-7
データバス
スクランブル
パターンメモリ
タンパ
検出
スイッチ
507
*WEPMD
A4-19
デコーダ
回路
605
バックアップ
用電池
*WE
*WEPMA

【書類名】　　要約書

【要約】

【課題】本発明は、ＣＰＵおよび内部デバイスを有する内部回路と、その内部回路に対し外付けされた外部デバイスを含む外部回路とを備えた処理装置等に関し、不正なアクセスや逆解析の防止を図る。

【解決手段】ＣＰＵ１０１と、内部デバイス１０２～１０５と、ＣＰＵ１０１と内部デバイス１０２～１０５とを結ぶとともに外部にまで延びるバスライン１１０とを含む内部回路１００、および、バスライン１１０の、外部に延びた部分１１０ａに外付けされた外部デバイス２０１～２０３，２１１～２１２を含む外部回路２００を備え、内部回路１００が、バスライン１１０の、外部への出入口に介在し、そのバスライン上のアドレスおよびデータを、外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部１２０を含む。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社